Universidad Nacional Autónoma de México

Facultad de Ingeniería
División de Ingeniería Eléctrica

Simulador de redes GNS3: estudio, pruebas con prácticas y propuesta de uso.

Modalidad de Titulación:
"TESINA"

Que para obtener el título de
INGENIERO EN COMPUTACIÓN

Presenta
MANUEL ALEJANDRO PONCE MONTERROSAS

Director de tesina: **Ing. AZAEL FERNÁNDEZ ALCÁNTARA**

México D.F. Año: 2014

Dedicatoria

Agradecimientos

Contenido

Capítulo 1. Introducción

1.1 Antecedentes

Muchas de las actividades que realizamos en nuestra vida diaria, requieren que contemos con cierta información para su realización, en la actualidad, mucha de esta la obtenemos a través de dispositivos que se encuentran conectados a las redes de comunicación de datos.

El crecimiento que han tenido estas redes ha sido muy acelerado en los últimos años, su industria a pesar de ser relativamente joven, comparada con otras industrias, ha alcanzado un nivel e importancia muy significativo en las tareas y vida diaria de los seres humanos, así como en su forma de relacionarse [1]. Sus inicios se remontan a principios de la década de los sesenta cuando J.C.R. Licklider, del MIT y director del programa de investigación informática de DARPA, escribió una serie de memorandos en los que detalla su concepto de "Red galáctica", en donde describe en forma de idea, la manera en que los equipos se comunican actualmente en la red.

En 1961 se publicó el primer documento sobre la teoría de conmutación de paquetes, escrito por Leonard Kleinrock, del MIT y el primer libro sobre el tema en 1964.

Con la idea de poder comunicarse usando paquetes en vez de circuitos, se dio un gran paso en las redes informáticas. El otro paso clave fue conseguir que los ordenadores hablasen entre sí. En 1965, el ordenador TX-2, en Massachusetts, se conectó con el Q-32, en California, mediante una línea telefónica conmutada de baja velocidad, creando la primera red de área amplia del mundo [2].

1.2 Definición del problema

Con la necesidad, cada vez más creciente, de transmitir información a varios destinos locales y remotos para modificar, actualizar y respaldar información de manera rápida y eficiente, se necesitan diseñar, implementar y administrar, cada vez más, sistemas de redes de datos.

Los estudiantes, profesores, administradores y diseñadores de las redes requieren de herramientas que los ayuden a estudiar y probar sus sistemas de una manera controlada, eficiente, económica y lo más apegada a la realidad a la que se enfrentan. Es por ello que surgieron los simuladores de redes de datos, lo que ha conllevado a que en el mercado exista un mayor número de programas de simulación, desde los de uso general hasta los más especializados.

Estas aplicaciones permiten a la gente que está involucrada en el tema de la redes, realizar el análisis de las mismas en un ambiente controlado de laboratorio.

A pesar de que hay varios simuladores, no todos cumplen con las necesidades específicas de los diferentes usuarios que manejan estas herramientas, además de que algunos de estos softwares requieren una previa capacitación para poder usarlos ya que no son tan intuitivos y fáciles de usar.

Como parte de las actividades que realicé por mi servicio social en el laboratorio de tecnologías emergentes de redes (NETLab), perteneciente a la DGTIC, surgió la necesidad de tener una herramienta de simulación de redes estable, que pudiese manejar el soporte IPv6 que se necesitaba para probar protocolos de ruteo en esta versión de IP, además de que tuviera un manejo fácil de aprender. También había la necesidad de tener casos de estudios mediante una serie de prácticas que pudieran apoyar en el aprendizaje de grupos de alumnos que tomaron cursos de IPv6 en esta dependencia y que sirvieran de base para medir la factibilidad de su uso.

1.3 Objetivos

Contar, mediante la búsqueda e investigación, con una herramienta de software para simular redes de datos de una forma estable.

Que el software con el que se cuente, sea libre, pueda manejar el soporte IPv4 e IPv6, tenga un fácil manejo y un amplio rango para realizar pruebas de simulación.

Así mismo, crear en base a esta herramienta, una serie de prácticas que puedan apoyar a profesores, alumnos y todas las personas que se relacionen con el tema de las redes, en el estudio y enseñanza de la configuración de los protocolos de ruteo, tanto con la versión 4 y 6 de IP, así como de la autoconfiguración y creación de túneles en IPv6.

A su vez, se espera proponer que estas prácticas se implementen en algún grupo de estudio de la Facultad de Ingeniería, para contribuir con un medio más de enseñanza que tienen los laboratorios de redes de datos de esta facultad.

1.4 Contribuciones

Se realizaron una serie de prácticas dirigidas a profesores, alumnos y todas las personas que se relacionen con el tema de las redes de datos, para que tengan una opción más con la cual puedan realizar pruebas con los protocolos de ruteo tanto con IPv4 como con IPv6. Las prácticas están elaboradas para trabajar con el simulador GNS3, van desde como instalar y configurar el software, hasta como crear túneles para IPv6 con autoconfiguración y ruteo.

Después de haber estudiado algunos simuladores, se encontró que el software GNS3 posee varias características a destacar, entre ellas que es libre, bastante completo, con un gran alcance (usable en distintos sistemas operativos), en constante desarrollo y actualización.

Por lo anterior, se escogió esta herramienta de simulación para desarrollar este trabajo; es verdad que existe una herramienta muy similar a GNS3, que es más popular en México y es más fácil su instalación y configuración, el Packet Tracer, pero carece de algunas funciones con las que cuenta el simulador objeto de este estudio, como pueden ser que es propietario, y tiene un menor rango para realizar simulaciones.

1.5 Estructura de la tesis

Este trabajo consta de ocho capítulos, los cuales se distribuyen de la siguiente forma:

Capítulo 1: Se muestra la introducción del trabajo en donde se presentan los antecedentes de las redes de datos, la definición del problema, objetivos, así como las contribuciones que tendrá.

Capítulo 2: Se presentan los conceptos básicos que todo estudioso de las redes de datos debe tener para poder realizar las prácticas propuestas, ya que se hace uso de las versiones del protocolo de Internet, IPv4 e IPv6.

Capítulo 3: El tercer capítulo contempla un estudio de los simuladores de redes, desde que son y como funcionan, hasta resultados de la realización de pruebas a algunos de estos.

Capítulo 4: El cuarto capítulo presenta el estudio hecho al software simulador propuesto, el GNS3, mencionando las ventajas y desventajas que ofrece al usuario.

Capítulo 5: Se hace una breve revisión de los protocolos de ruteo.

Capítulo 6: En este capítulo se incluyen las prácticas que se proponen en este trabajo.

Capítulo 7: Para el siete se muestran las pruebas y los resultados de la aplicación de las prácticas en casos reales con estudiantes de dos grupos, donde se comprobó su funcionalidad y ayudó a detectar los problemas que pudieran experimentar los alumnos.

Capítulo 8: Finalmente en este capítulo, se presentan las conclusiones a las que se llegaron.

Capítulo 2. Conceptos básicos

2.1 Introducción

La necesidad de tener los conceptos básicos claramente entendidos, es que a partir de ellos se pueda comprender, de una mejor manera, los temas que vendrán posteriormente y así avanzar más rápidamente en su estudio y análisis.

Se presentan cuatro temas fundamentales que son necesarios para poder comprender claramente los capítulos centrales de este trabajo, los conceptos van desde el modelo OSI hasta el protocolo de Internet versión seis (IPv6).

2.2 Modelo OSI

El Modelo OSI fue creado por la Organización Internacional para la Normalización (ISO, por sus siglas en inglés), en 1984, como una forma de poder dividir el proceso de transmisión de la información entre equipos informáticos en capas, donde cada una de estas se encarga de ejecutar una determinada parte del proceso [3].

Al organizar el procedimiento en capas, se hace más sencillo comprender la acción que se produce durante la comunicación que hay entre los protocolos de aplicación de dos dispositivos que se estén comunicando, ayudando así a los diseñadores de redes a implementar los mismos de una manera más organizada.

Son siete las capas de este modelo de referencia, cada una de las cuales realiza una función de red específica. A esta forma de dividir las funciones se le denomina “división en capas” [4].

Utilizar las capas del modelo OSI, brinda las siguientes ventajas:

- *Divide la comunicación de red en partes más pequeñas y sencillas de entender.*
- *Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes*

- *Permite a los distintos tipos de hardware y software de red comunicarse entre sí.*
- *Impide que los cambios en una capa puedan afectar a las demás capas, ayudando a que se puedan desarrollar con más rapidez.*

Las siete capas del modelo de referencia OSI son las que se muestran en la figura 1:

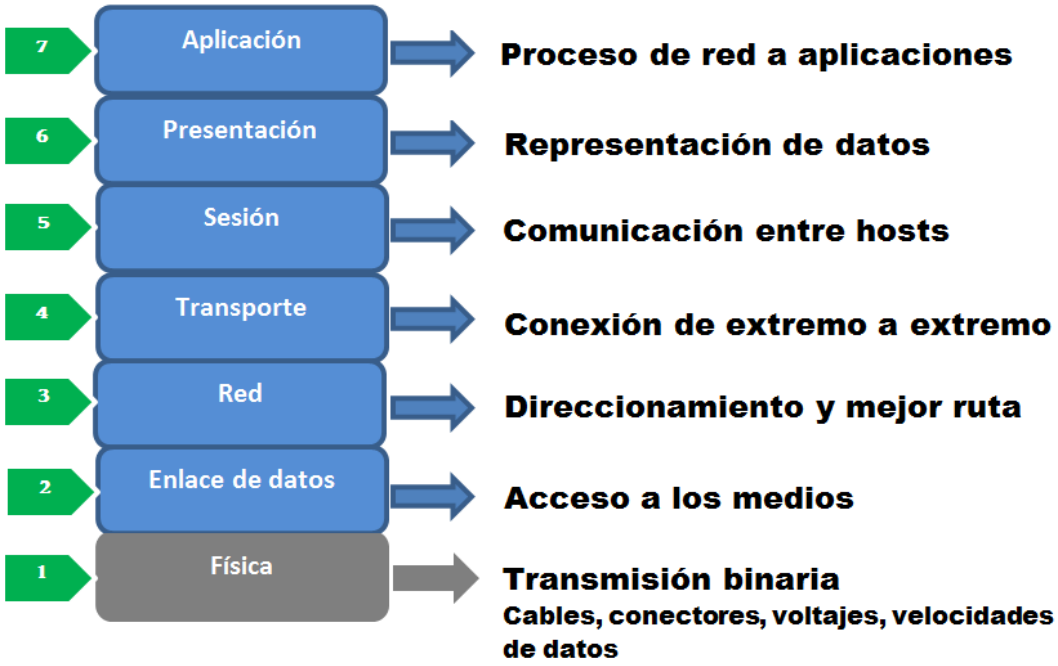


Figura 1. Las siete capas del modelo OSI y su función [5].

2.3 Pila de Protocolos TCP/IP

TCP/IP es un conjunto de protocolos. La sigla TCP/IP significa "Protocolo de Control de Transmisión/Protocolo de Internet". Proviene de los nombres de dos protocolos importantes del conjunto de protocolos, es decir, del TCP y del IP.

La pila de protocolos es una colección ordenada de protocolos organizados en capas, fue desarrollada después de que la red se volviera operacional por un dedicado grupo de representantes de la industria de la informática del Reino Unido, Francia y Estados Unidos, el cual, tenía la tarea de crear un sistema abierto y de múltiples capas, que permitiría a los

usuarios de todo el mundo intercambiar datos de forma sencilla y con ello dar una apertura a nuevas posibilidades de colaboración y de comercio. Estos protocolos fueron adoptados como normas militares en 1983 y todos los nodos conectados a la red se convirtieron a los nuevos protocolos. Al mismo tiempo de que TCP/IP fue adoptado como una norma, el término Internet comenzó a ser utilizado de manera común [6].

La popularidad de TCP/IP creció rápidamente ya que este modelo fue la base para la conexión a Internet, además de ser un conjunto de protocolos de norma abierto, ser independiente de la conexión física de la red (Ethernet, DSL, dial-up, fibra óptica, inalámbrica y cualquier otro medio de transmisión), así como su compatibilidad con diferentes sistemas operativos y hardware; se utiliza un esquema de direccionamiento común que permite a cualquier interfaz de un dispositivo tener una dirección global única que cualquier otra interfaz en otro dispositivo en la red entera. Inclusive es posible emplearlo en redes que no tienen conexión a Internet y una estandarización en los protocolos de capa superior.

Arquitectura de TCP/IP

La arquitectura de la pila TCP/IP está compuesta de menos capas que las siete utilizadas en el modelo OSI, las 4 capas utilizadas se ilustran en la figura 2.

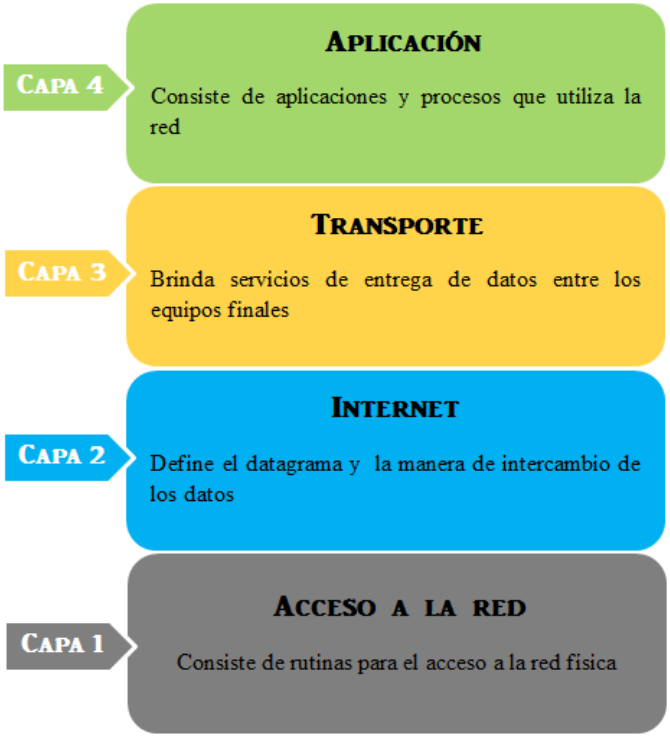


Figura 2. Las capas del modelo TCP/IP y su función [7].

Como en el modelo OSI, los datos pasan desde una capa superior hacia una inferior de un nodo origen, es decir, de la capa de aplicación hasta llegar a la capa de acceso a red. Cada capa de la pila agrega controles a la información para garantizar la apropiada entrega; este control de información es llamado encabezado, porque es colocado frente a los datos que serán transmitidos. Cada capa trata toda la información que recibe como datos y le agrega su propio encabezado al principio de la información, esto también es conocido como encapsulado. Cuando los datos se reciben del nodo destino, cada capa quita su encabezado de los datos hasta llegar a la capa de aplicación, la cual interpreta los datos (ver figura 3).

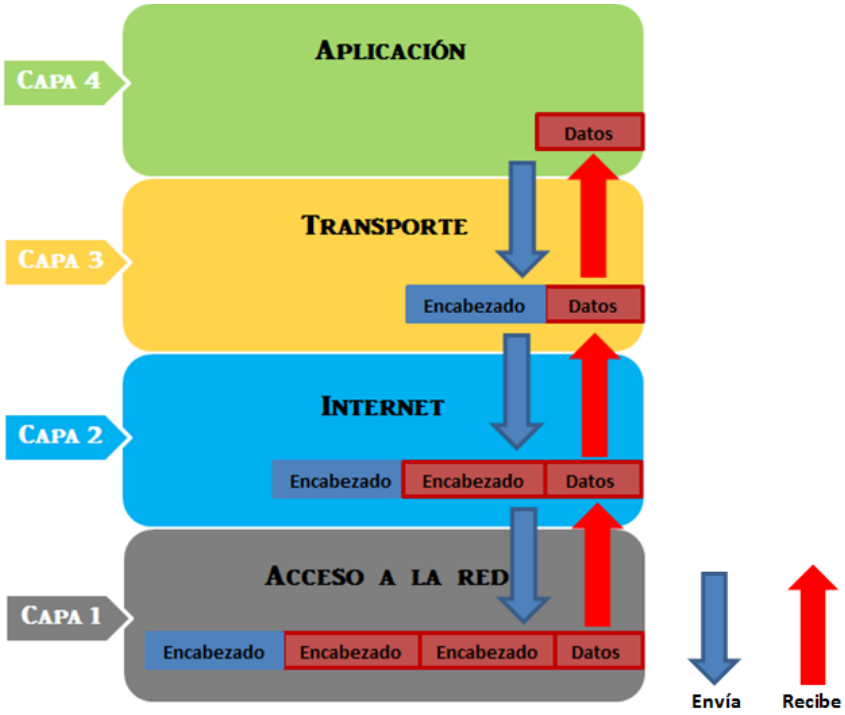


Figura 3. Encapsulamiento de los datos a través de las capas de TCP/IP [8].

Cada capa tiene su propia estructura de datos, la cual está diseñada para ser compatible con las capas que la rodean y con las capas similares a ellas de los nodos vecinos.

2.4 Protocolo de Internet versión 4 (IPv4)

La primera versión del Protocolo de Internet (IP o Internet Protocol) que ha sido usada a gran escala y que actualmente todavía está en uso, es la versión 4 y se le conoce como IPv4.

IPv4 es un protocolo que permite que cualquier dispositivo con acceso a Internet (PC, notebook, smartphone, tableta, etc.) pueda conectarse a una red a través de un número de identificación llamado dirección IP, para poder enviar y recibir datos con otros equipos.

El propósito principal de este protocolo es proveer una dirección única a cada interfaz de un sistema en el contexto correspondiente, para asegurar que una computadora en una red pueda identificar a otra en la misma o en otra red, local o remota [9].

Las direcciones IPv4 se escriben en notación decimal, en campos separados con puntos, utilizando direcciones de 32 bits (8 bytes) como por ejemplo, 132.248.10.7. Estas

direcciones se encuentran en el rango entre 0.0.0.0 y 255.255.255.255. Son direcciones únicas que llegan hasta 4, 294, 967, 296, de las cuales se reservan muchas direcciones para las redes privadas, para redes llamadas de multidifusión, y otras. Lo anterior quiere decir que el número antes escrito se reduce y limita más la posibilidad de asignar direcciones IP.

Este protocolo es el más utilizado en la capa de red del modelo OSI. Fue descrito inicialmente en la solicitud de comentarios (RFC, por sus siglas en inglés) 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (IETF, por sus siglas en inglés), en septiembre de 1981, documento que dejó obsoleto al RFC 760 de enero de 1980 [10].

Arquitectura de clases de red (Classful network architecture)

En esta arquitectura hay tres clases principales de direcciones IPv4 que se asignan dependiendo del tamaño de las organizaciones, a estas clases se les conoce como: clase A, clase B y clase C.

Existen dos clases más que son la clase D, que se utiliza para grupos de Multicast y la clase E que se reserva para fines de investigación solamente (ver tabla 1).

Tabla 1. Clases de direcciones en IPv4.

Clase	**Rango**	**# Redes**	**# Hosts**	**Máscara en decimal**
A	0.0.0.0 – 127.255.255.255	128	2^{24}-2= 16777214	255.0.0.0
B	128.0.0.0 – 191.255.255.255	16384	2^{16}-2= 65534	255.255.0.0
C	192.0.0.0 – 223.255.255.255	2.097.152	2^{8}-2= 254	255.255.255.0
D	224.0.0.0 – 239.255.255.255			
E	240.0.0.0 – 255.255.255.255			

Direcciones IPv4 en formato CIDR

Ya desde hace más de 10 años, la IETF desarrolló las direcciones CIDR (Classless Inter-Domain Routing) como una solución a mediano y largo plazo para la escasez de direcciones IPv4 y como solución a la falta de capacidad en las tablas de enrutamiento de Internet globales.

Redes privadas

De los más de cuatro mil millones de direcciones teóricamente posibles con IPv4, tres rangos están especialmente reservados para utilizarse solamente en redes privadas (ver tabla 2). Estos rangos no tienen encaminamiento fuera de una red privada y las máquinas dentro de estas redes no pueden comunicarse directamente con las redes públicas. Pueden, sin embargo, comunicarse hacia redes públicas a través del mecanismo de traducción de direcciones de red llamado NAT (Network Address Translation).

Tabla 2. Bloque de direcciones IPv4 para redes privadas.

Nombre	Rango de direcciones IP	Número de direcciones IP	Tipo de clase	Bloque CIDR mayor
Bloque de 24 bits	10.0.0.0 – 10.255.255.255	16,777,215	Red simple clase A	10.0.0.0/8
Bloque de 20 bits	172.16.0.0 – 172.31.255.255	1,048,576	16 redes clases B contiguas	172.16.0.0/12
Bloque de 16 bits	192.168.0.0 – 192.168.255.255	65,535	256 redes clases C contiguas	192.168.0.0/16

Anfitrión local (Localhost)

Además de las redes privadas, el rango 127.0.0.0 – 127.255.255.255 o 127.0.0.0/8 en la notación CIDR, está reservado para la comunicación del host local (localhost o loopback).

Ninguna dirección de este rango deberá aparecer en una red, sea pública o privada, y un paquete enviado hacia cualquier dirección de este rango deberá regresar como un paquete entrante hacia la misma máquina.

2.5 Protocolo de Internet versión 6 (IPv6)

Cuando se diseñó IPv4 no se pensó que pudiera llegar a tener tanto éxito comercial el uso de Internet y un imparable crecimiento de usuarios y dispositivos conectados a la red, es

por eso que se pensó que 2^{32} direcciones en la teoría, es decir, 4, 294, 967, 296 direcciones alcanzarían de sobra sin embargo, esa cantidad si vislumbró insuficiente años después.

Por este motivo y previendo la situación de agotamiento acelerado, en el organismo que se encarga de la normalización de los protocolos de Internet (IETF), después de varias propuestas se definió lo que actualmente es conocido como IPv6 (Protocolo de Internet versión 6), que posee direcciones con una longitud de 128 bits, es decir 2^{128} posibles direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456), o dicho de otro modo, 340 trillones de trillones de direcciones disponibles.

Una dirección IPv6 (128 bits) se representa mediante ocho campos de cuatro dígitos hexadecimales, cada campo representado con 16 bits (dos octetos). Los campos se separan mediante dos puntos ":".

En un formato básico de una dirección IPv6, por lo general, los tres campos más significativos que están a la izquierda (48 bits) contienen el **prefijo global de ruteo**, el campo siguiente (16 bits) es para el **ID de la subred** y los cuatro campos menos significativos situados a la derecha (64 bits) contienen el **ID de interfaz** [11] (ver figura 4).

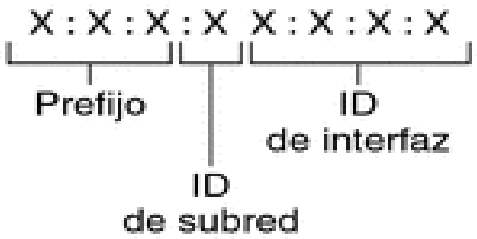


Figura 4. Formato básico de una dirección IPv6.

Un ejemplo de dirección IPv6 podría ser:

2001:0db8:85ª3:0000:0000:8ª2e:0370:7334

Los ceros iniciales (del lado izq.) de cada grupo pueden omitirse, aunque cada grupo debe contener al menos un dígito hexadecimal. De ese modo, la dirección IPv6 ejemplo podría escribirse:

2001:db8:85ª3:0:0:8ª2e:370:7334

A su vez se permite utilizar la notación de dos puntos consecutivos ": :" para representar campos contiguos de ceros, quedando la dirección ejemplo inicial de la siguiente manera:

2001:db8:85ª3::8ª2e:370:7334

El despliegue de IPv6 se ha ido realizando gradualmente, en una coexistencia ordenada con IPv4, al que irá desplazando a medida que dispositivos de clientes, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet. Por ello, es importante que se entienda cómo se realiza el despliegue de la versión más reciente del protocolo de Internet, tanto si se es usuario residencial, como corporativo, proveedor de contenidos, proveedor de servicios de Internet, así como la propia administración pública. En la siguiente tabla 3 se presenta un resumen de ambas versiones.

Tabla 3. Comparación de algunas características entre IPv4 e IPv6 [12].

IPv6	**IPv4**
Direcciones de 128 bits (16 bytes) en notación hexadecimal	Direcciones de 32 bits (4 bytes) en notación decimal
Arquitectura jerárquica de direccionamiento	Arquitectura plana / jerárquica de direccionamiento
Configuración automática de direcciones	Configuración manual de direcciones
Direcciones Multicast y Anycast	También Broadcast
Soporte de seguridad integrada (IPSec) (No obligatorio en su uso)	Soporte de seguridad adicional (IPSec) (No obligatorio en su uso)
Con identificación QoS	Sin identificación QoS
Las direcciones IPv6 se asignan a interfaces lógicas	Las direcciones IPv4 se asignan a interfaces físicas
Fragmentación de paquetes sólo en el origen	Fragmentación de paquetes en nodos intermedios

Tipos de direcciones IPv6

- **Unicast**.- Es utilizado para identificar la interfaz de un nodo. Un paquete enviado a una dirección de este tipo es entregado únicamente a la interface identificada por esa dirección.

- **Anycast**.- Se asigna a varias interfaces (usualmente en múltiples nodos). Un paquete enviado a una dirección de este tipo es entregado a una de estas interfaces, usualmente al destino más cercano.

- **Multicast**.- Utilizado para identificar a un grupo de interfaces. Un paquete enviado a una dirección de este tipo es recibido y procesado por todos los miembros del grupo Multicast.

Existen en IPv6 prefijos que no son ruteables, estos son conocidos como "Improper routes" mostrados en la tabla 4, de acuerdo a la IANA [13].

Tabla 4. Prefijos que no deben ser ruteados.

Notación IPv6	Tipo de dirección
::/128	No especificada
::/96	Reservada por la IETF [14]
::1/128	Loopback
::ffff:0:0/96	Mapeadas-IPv4
0100::/8	Discard-only prefix [15]
2001:0002::/48	BMWG
2001:10::/28	ORCHID
2001:DB8::/32	Para documentación
FE80::/10	Unicast de enlace local
FEC0::/10	Reservada por IETF
3FFE::/16	6Bone [16]

Otros prefijos que se definen en su alcance (ver tabla 5):

Tabla 5. Prefijos cuyo ruteo se define en el alcance (scope) [17].

Notación IPv6	Tipo de dirección
2001:0000::/32	Teredo
2002::/16	6to4
FC00::/7	Local Única
FF00::/8	Multicast

Autoconfiguración en IPv6

Existen dos tipos de autoconfiguración en IPv6 los cuales son los siguientes:

Sin estado (Stateless): donde un ruteador participa en la configuración de la dirección IPv6 de cada host.

- **Con estado (Stateful)**: un servidor de DHCP IPv6 es el encargado de configurar la dirección IPv6 en cada host.

Mecanismos de Transición

- **Capa IP dual**: los nodos (ruteadores, switches, etc. y los hosts) soportan IPv4 e IPv6 simultáneamente y por tanto se crean segmentos de red también duales (ver figura 5).

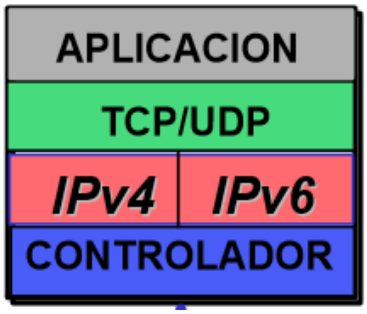


Figura 5. Esquema de soporte del mecanismo de transición IP dual [18].

- **Encapsulamiento** (Túnel): los paquetes IPv6 se encapsulan con encabezados de IPv4 para transportarse por redes de IPv4. Existen los túneles configurados manualmente y los automáticos [19] (ver figura 6).

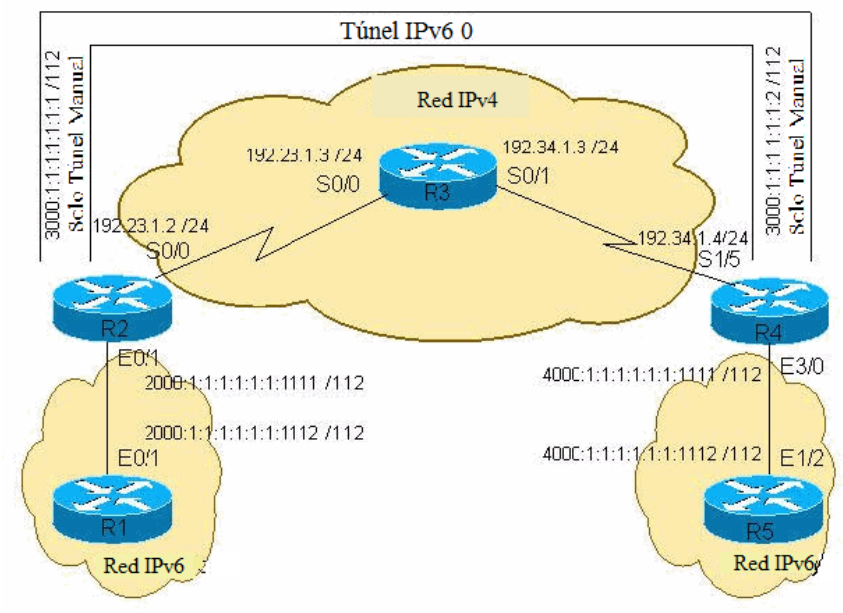


Figura 6. Esquema del mecanismo de transición de encapsulamiento [20].

- **Traducción**: consiste en la traducción de paquetes IPv4-IPv6 en ambos sentidos (ver figura 7).

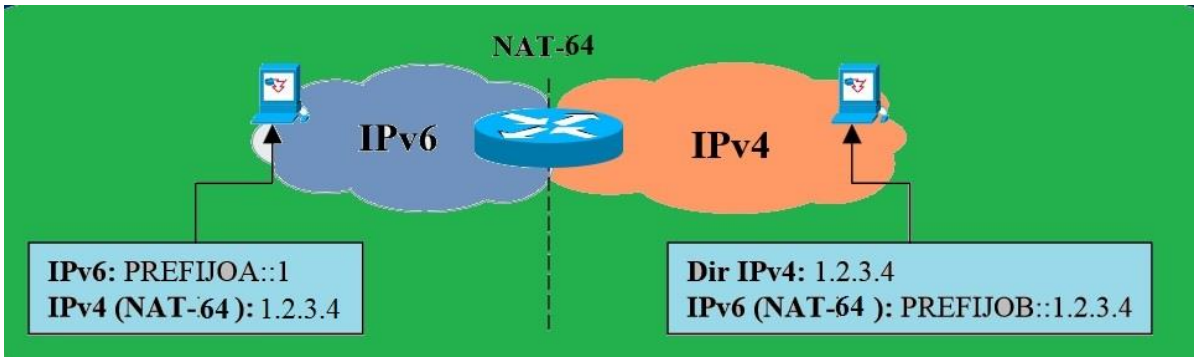


Figura 7. Esquema del mecanismo de transición de traducción mediante NAT-PT.

Capítulo 3. Simuladores de Redes

3.1 Introducción

Los simuladores de redes permiten crear un marco para la práctica y la exploración en un ámbito sin riesgos, analizar esquemas de redes desde diferentes perspectivas e integrar conocimientos aprendidos con anterioridad.

En este capítulo se presenta un breve estudio hecho a unos de los principales simuladores de redes que existen en la actualidad, analizando sus características y realizando algunas pruebas de funcionamiento a tres de estos simuladores.

3.2 Definición y funcionamiento

Simuladores de redes

De acuerdo con el diccionario de la lengua española, simular significa representar algo, fingiendo o imitando lo que no es, por lo que podría definirse a la simulación como la experimentación con un modelo en un determinado intervalo de tiempo, que imita ciertos aspectos de la realidad.

El simular permite trabajar con un modelo en condiciones similares a las reales, pero con variables controladas; aunque está creado o acondicionado artificialmente, permite probar el comportamiento de una persona, de un objeto o de un sistema en ciertos contextos muy parecidos a los reales, para que así, se pueda predecir el impacto que tendrá el mismo y corregir fallos, si existieran, antes de que la experiencia se concrete en el plano de lo real [21].

Los simuladores de redes son programas para diseñar topologías de red en forma virtual, que van, desde las más pequeñas hasta las más complejas; la complejidad depende tanto de que tan potente sea el simulador para permitirnos crear grandes topologías con un

gran número de dispositivos, como de los recursos del equipo en el que se esté desarrollando dicha simulación.

Estas herramientas permiten reproducir condiciones específicas en un entorno virtual y controlado, como picos muy altos de tráfico en la red y ver las consecuencias que tendrían estas sobre el conjunto.

Ventajas de la Simulación

- ✓ Un estudio de simulación ayuda a entender como opera un sistema, no como se cree que opera.
- ✓ Ayuda en los cuellos de botella y puntos de congestión, indicando donde los procesos están siendo retrasados en exceso.
- ✓ Cuando se implementen nuevos procedimientos, reglas, políticas y flujos de información, pueden ser probados sin interrumpir las operaciones del sistema real.
- ✓ El tiempo puede ser comprimido o expandido permitiendo un aumento o disminución de la velocidad de los fenómenos en investigación.
- ✓ Se pueden probar nuevas hipótesis en la red sin que se tenga que parar a la misma o exponer los datos a pérdidas.

Desventajas de la Simulación

- ✓ Que el programa de simulación no soporte todas las variables y casos de operación de una red muy grande.
- ✓ Los resultados de la simulación pueden ser difíciles de interpretar.
- ✓ No cualquiera puede manejar un software de simulación para construir los modelos a probar, requiere de una cierta preparación.

3.3 Simuladores de red existentes

Network Simulation and Prototyping Testbed (NEST)

Es un entorno gráfico, introducido por el departamento de ciencias de la computación de la universidad de Columbia, para la creación de forma rápida de simulaciones de sistemas de redes distribuidas y probar protocolos básicos de red, bases de datos distribuidas y sistemas operativos así como fabricación de sistemas distribuidos.

Creado para plataformas Unix, permite al usuario modificar y reconfigurar una simulación en el momento en el que se está ejecutando, lo que ayuda a estudiar la respuesta dinámica que tendrá el sistema a posibles fallas y cargas espontaneas de trabajo, ya que los cambios realizados se activan casi de forma instantánea en la simulación.

NEST está organizado bajo la arquitectura cliente/servidor, donde el llamado **servidor de simulación** es el responsable de la ejecución de los escenarios de la simulación y los **monitores cliente** son los que se encargan de reconfigurar y controlar la simulación, los cuales pueden, y comúnmente, residen en máquinas separadas del servidor. Esto ayuda a que el servidor solo dedique sus recursos a ejecutar la simulación mientras que delega a las estaciones de trabajo el control y la presentación de la simulación, permitiendo así la distribución del simulador sobre un entorno de red y el desarrollo de un banco de pruebas compartido (ver figura 8).

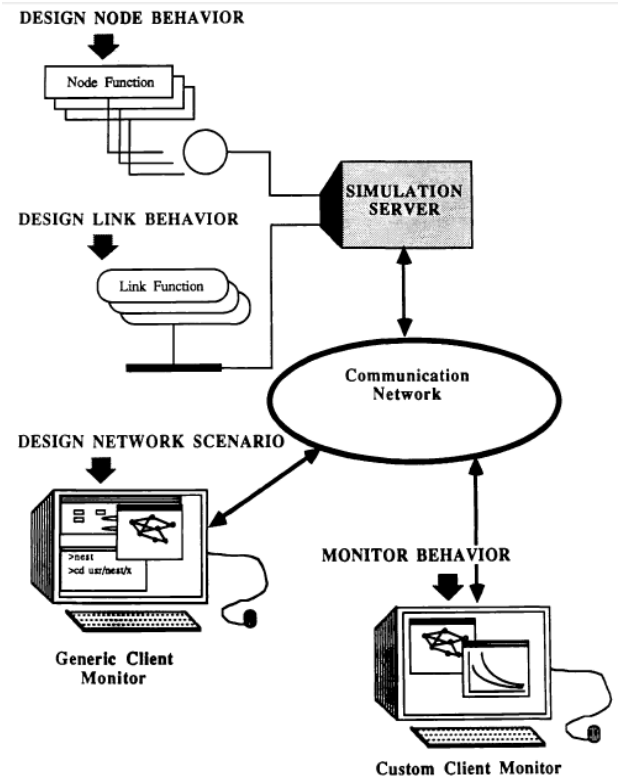


Figura 8. Arquitectura de NEST. Imagen tomada de la referencia [22].

Las funciones que tendrá la simulación se codifican en el lenguaje C, lo que permite a los usuarios ejecutar sus propios códigos hechos en este lenguaje.

Los usuarios pueden controlar y gestionar una simulación a través de herramientas gráficas de monitoreo estándar en la interfaz del programa, dando clic con el ratón en el menú de generar nodos se crean los mismos y arrastrando el ratón desde un nodo a otro se crean los vínculos de estos.

Una vez que el usuario define un escenario de simulación, este se envía al servidor de simulación donde se carga y se ejecuta.

De acuerdo a la documentación, este simulador logra una eficiencia de recursos significativa mediante el uso del modelo de ejecución multi-hilo y el procesamiento de uno a la vez a través del uso de un planificador optimizado. Este modelo implica una cantidad mínima de sobrecarga en un cambio de contexto a diferencia de la carga que tendría un enfoque basado en multitareas [22].

Maryland Routing Simulator (MaRS)

Es un discreto simulador de redes desarrollado por la universidad de Maryland el cual, provee una plataforma con la que se pueden realizar pruebas y comparaciones de algoritmos de protocolos de ruteo mediante el diseño y configuración de redes simuladas. Está definido bajo variables de estado y eventos.

Una simulación en MaRS básicamente consiste en un conjunto de tres elementos:

- Una red física
- Un algoritmo de ruteo
- Y una carga de trabajo.

Adicionalmente, puede contener dos elementos más: un **monitor de rendimiento**, el cual lleva a cabo las medidas del rendimiento y comparación de los diferentes algoritmos de ruteo, y un **componente de suspensión** en donde se pueden definir las condiciones en las cuales la simulación deba terminar.

MaRS también tiene la ventaja de que si alguno de sus componentes no satisface alguna tarea o propósito deseado, el usuario puede definir un nuevo componente ajustándolo a sus necesidades específicas.

Puede ser ejecutado con o sin un sistema Windows, cuando se ejecuta en Windows se tiene una interfaz gráfica para diseñar y configurar las redes, cuando no, la ejecución de este es más rápida. Los componentes del simulador son los siguientes (ver figura 9):

- Enlace
- Nodo
- Ruteo
- Función del costo de enlace
- Carga de trabajo
- Monitor de rendimiento
- Componente de suspensión

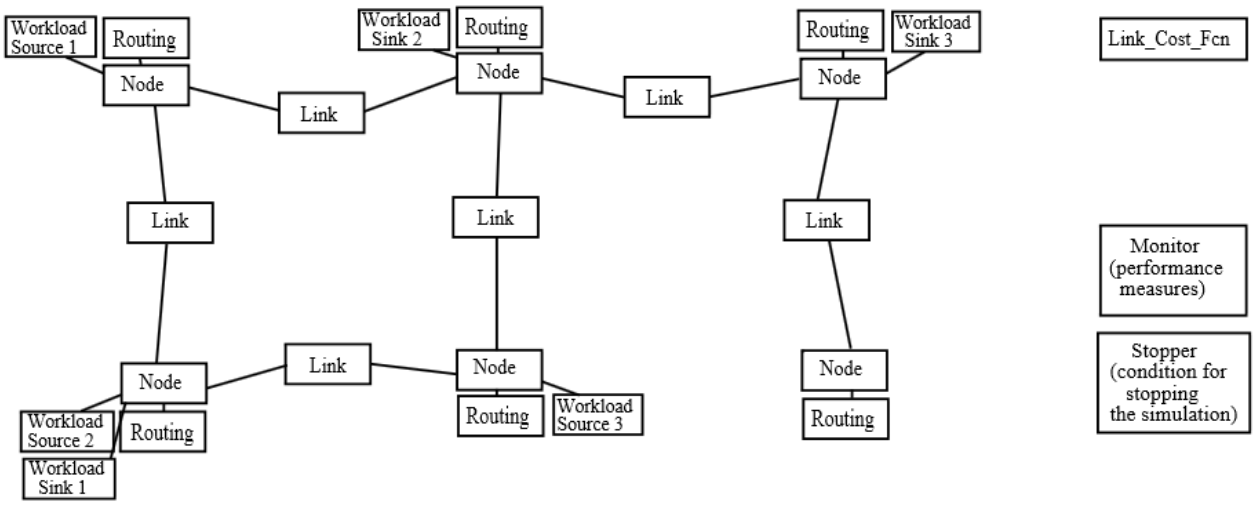


Figura 9. Ejemplo de los componentes que se usan en una simulación en MaRS [23].

Scalable Simulation Framework (SSF)

Es un simulador realizado en el lenguaje C++ con el respaldo de la corporación Renesys, el instituto para el estudio de la tecnología de seguridad en Dartmouth y DARPA. Incorpora dos interfaces de programación en los lenguajes Java y C++.

Se basa en 5 paquetes de clases que son:

- Entity
- inChannel
- outChannel
- Process
- Event

Con estos paquetes el simulador permite al usuario modelar su sistema, y su interacción con la simulación se hace a través del lenguaje para modelado DML (ver figura 10).

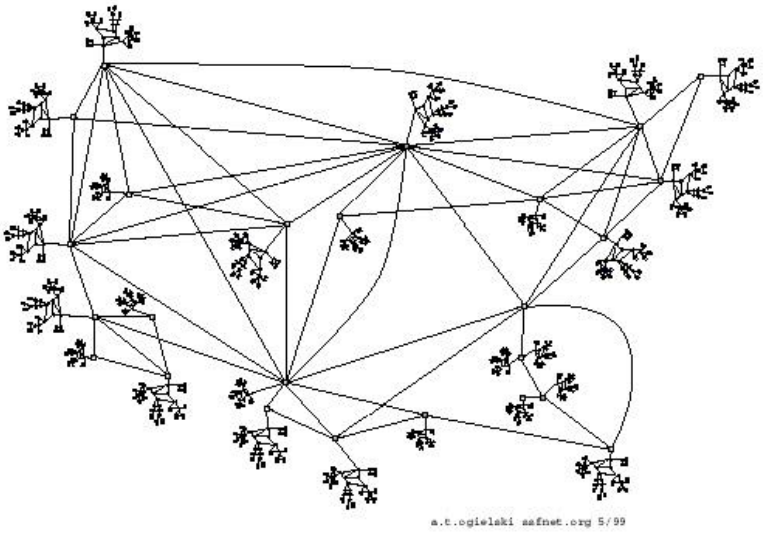


Figura 10. Ejemplo de la creación de un complejo modelo de red con DML en el simulador SSF. Imagen tomada de la referencia [24].

De acuerdo con la documentación, es altamente escalable y permite el uso de prácticamente todos los protocolos en Internet [24].

Una desventaja que presenta este simulador es que la versión más optimizada es la comercial y las versiones gratuitas no tienen un adecuado rendimiento en sus simulaciones, sobre todo en las más complejas.

Java Simulator (J-Sim)

J-Sim (anteriormente conocido como JavaSim) es un entorno de simulación desarrollado totalmente en Java con la ayuda de NSF, DARPA, Cisco y las universidades de Illinois y Ohio.

La entidad básica en este simulador son los componentes y su comportamiento está definido en términos de contratos, donde la arquitectura de componentes autónomos imita la arquitectura de diseño de los circuitos integrados de la manera más cercana posible.

J-Sim también proporciona una interfaz de secuencias de comandos para permitir la integración con diferentes lenguajes de script como Perl , Tcl o Python. Usa la herramienta **gEditor** para crear la interfaz gráfica del simulador, que se debe instalar después de J-sim.

La extensión para usar J-Sim con Tcl se llama Jacl. A diferencia del simulador siguiente, el Ns-2, en J-Sim las clases, métodos y campos necesitan ser exportados explícitamente para ser accedidos en el ambiente Tcl (ver figura 11).

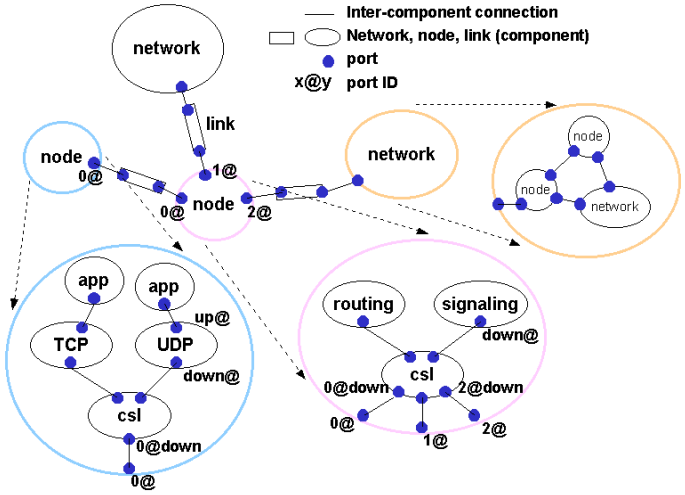


Figura 11. Esquema de un escenario de red en el simulador J Sim. Imagen tomada de la referencia [25].

Proporciona soporte para la gran mayoría de los protocolos usados en Internet, así como Multicast y QoS [25].

Network Simulator 2 (ns-2)

Es un simulador de eventos discretos orientado a redes, escrito en C++ que surgió a finales de los años 80, usa OTcl, una variante Orientada a Objetos de Tcl, para poder crear la comunicación con el usuario. Se desarrolló como una variante del simulador de redes **Real.**

Más adelante la agencia DARPA participó en el proyecto que desarrolló al simulador con el proyecto VINT, también se encuentra patrocinado por la empresa Xerox y el instituto de ciencias de la información de la universidad del sur de California [26].

Tiene la capacidad de simular protocolos de ruteo Unicast y Multicast en redes estructuradas e inalámbricas.

Este simulador en sus inicios estaba pensado para ejecutarse solo en una plataforma Linux, sin embargo, más adelante se desarrolló una versión sobre Windows.

Está compuesto de dos jerarquías, la compilada escrita en C++ y la interpretada que corresponde a OTcl, ambas se encuentran estrechamente relacionadas entre sí, ya que cada objeto presente en la jerarquía compilada encuentra su símil en la jerarquía interpretada. Cuenta con un visualizador llamado **Nam**, que permite ver en forma más cómoda los resultados de la simulación.

En la siguiente figura número 12 se muestra la arquitectura interna de ns-2.

Figura 12. Arquitectura interna del simulador ns2 [27].

Realistic And Large Network Simulator (Real)

Es un simulador diseñado para estudiar el comportamiento dinámico que tienen las redes de datos en sus flujos de información y así diseñar un esquema de control de la congestión, que se genera en la transferencia de datos por medio de la implementación de una red virtual que simule el comportamiento que tiene la versión física.

El simulador cuenta con una interfaz gráfica (GUI) hecha en Java en la universidad de Cornell para facilitar el diseño de los escenarios. A sí mismo, sus módulos fueron realizados en el lenguaje C.

No permite el estudio de sistemas o parámetros que no afecten de forma directa al flujo principal de conexiones TPC/IP, lo que limita la capacidad de modelar un sistema real.

NCTUns 2.0 Network Simulator/Emulator

Este programa es tanto un emulador como un simulador desarrollado en la universidad de Harvard. Para darle un mayor desempeño a la simulación, el programa utiliza el mismo TCP/IP que se encuentre en la computadora donde se realiza la simulación, además de usar todas sus herramientas sin ninguna modificación (por ejemplo, herramientas de monitoreo y configuración de redes).

Algunos de los tipos de redes que se pueden simular son las estructuradas con hosts fijos, LAN wireless, redes OBS, entre otras.

Cuenta con los dispositivos de hubs, switches, ruteadores, hosts, estaciones, puntos de acceso, estaciones base GPRS, switches ópticos, etc.

Las normas, protocolos y protocolos de aplicación que se pueden usar son: IEEE 802.3 CSMA/CD MAC, IEEE 802.11 (b) CSMA/CA MAC, IP, IP móvil, Diffserv (QoS), RIP, OSPF, UDP, TCP, HTTP, FTP, telnet, etc. Así mismo, el software provee una GUI que ayuda al usuario a diseñar y configurar la red con la que se va a trabajar, definir caminos para nodos móviles, dibujar gráficos del desempeño de la red, ver animaciones, entre otras cosas. La interfaz es muy completa solo que tiene una distribución un tanto confusa de las opciones y menús. Las simulaciones también se pueden realizar por medio de un script (ver figura 13).

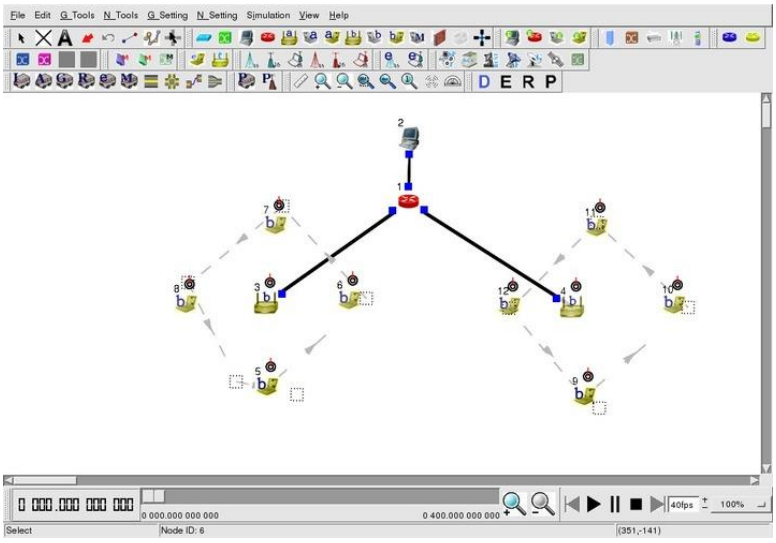


Figura 13. Área de trabajo en el simulador NCTUns 2.0 [28].

Packet Tracer

"Cisco Packet Tracer" es un programa de simulación de redes muy conocido, que permite a los estudiantes de las TIC experimentar el comportamiento de las redes mediante la creación, diseño, simulación, visualización y evaluación de topologías de red.

Está disponible de forma gratuita oficialmente sólo para instructores, estudiantes, exalumnos y administradores que están registrados en "Networking Academy" de Cisco [29]. Actualmente es usado en la facultad de Ingeniería de la UNAM.
Permite crear una red con un gran número de dispositivos, fomentando la práctica, el descubrimiento y la solución de problemas, al aplicar conceptos técnicos y diseño de sistemas de redes.

Las topologías de red en este simulador se crean arrastrando los dispositivos que se encuentran del lado inferior izquierda de la ventana principal al área de trabajo del software, así por ejemplo, dando clic en ellos, se puede ingresar a sus consolas de configuración donde están soportados casi todos los comandos del Cisco OS. Sin embargo, tiene algunas limitaciones como el no tener la funcionalidad del soporte completo de IPv6.

OPNET IT Guru Academic

Es un simulador en el cual se pueden diseñar, en base a modelos preconstruidos de protocolos y dispositivos, topologías de red para verificar el comportamiento de estas bajo ciertas condiciones de carga que se especifiquen.

Fue creado para la enseñanza de redes a un nivel de básico a intermedio, por lo cual es más usado en el ámbito académico, como es el caso de la facultad de Ingeniería.

Los protocolos y dispositivos que se incluyen en esta versión del simulador son fijos, no se pueden crear nuevos ni modificar el comportamiento de los ya existentes, además se limita a simular un cierto número de eventos y no permite tener grandes cantidades de dispositivos en una sola simulación [30].

Existe una versión de este software llamada **OPNET Modeler** que no tiene las limitaciones con las que cuenta la versión de *academic* y dispone de más herramientas para poder crear simulaciones sofisticadas, permitiendo modificar las características de los protocolos y dispositivos que se incluyen. Sin embargo, su gran inconveniente es que no es gratuita, se tiene que pagar una licencia para obtenerla, aunque permite usar tecnologías más recientes en el ámbito de las redes como son IPv6, MPLS y OSPFv3.

3.4 Pruebas de funcionamiento de algunos simuladores

Se realizaron algunas pruebas de funcionamiento a los simuladores: Java Simulator (J-Sim), Network Simulator 2 (ns-2) y Packet Tracer. Los resultados obtenidos de las pruebas se listan en la tabla 6, mostrando de una manera resumida, algunas características importantes que son de interés para los fines de este trabajo.

Tabla 6. Aspectos analizados en los simuladores probados.

Característica	J-Sim	ns-2	Packet Tracer
Disponibilidad	Es fácil conseguirlo desde su página oficial de manera gratuita, donde se encuentra junto con los parches que son necesarios para su correcta instalación y ejecución.	Disponible de forma sencilla y gratuita en su sitio oficial, donde se encuentra el código fuente solo o el "all in one", que es el paquete que contiene el código fuente y todas las librerías extras que necesita el simulador.	Este software por requerir una licencia de uso, solo está disponible de forma gratuita, oficialmente para personas que estén registrados en el programa "Networking Academy" de Cisco.
Interfaz gráfica	Es una interfaz muy intuitiva, donde muestra la estructura de la simulación en una ventana del lado izquierdo de la pantalla, con el menú de componentes y herramientas en la parte superior. También utiliza una ventana de consola.	Se pueden observar de forma clara y precisa los paquetes que son enviados entre los elementos, así como saber cuáles son los que no pueden ser procesados y son descartados.	Cuenta con una interfaz intuitiva y amigable. Se puede diseñar una topología usando el ratón de la PC. Sus menús de herramientas, dispositivos y conectores están a la vista y arrastrando el elemento deseado al área de trabajo, éste se agrega a la topología que se desee diseñar.

Ventajas	El editor gráfico facilita mucho crear y probar una simulación ya que se asemeja mucho a otros entornos gráficos de otros simuladores existentes en el mercado,	Su programación es orientada a objetos, lo que flexibiliza y simplifica la tarea de la programación de las simulaciones.	Las pruebas en esta herramienta se realizan con relativa facilidad, incluso para usuarios no muy especializados en las redes, para topologías sencillas.
Desventajas	Sus componentes son jerárquicos, por lo cual si se realiza un cambio en un componente afectará la relación que tiene con otros componentes.	Se requieren conocimientos básicos de programación en OTcl, lo cual reduce la cantidad de usuarios que pueden utilizar este simulador. El realizar un escenario de pruebas no resulta tan sencillo ya que se tiene que programar todo lo que se desee simular.	No soporta todos los comandos que se usan en un ruteador real de Cisco.
Escalabilidad	La versión que se probó es la 1.3 liberada en el 2005 y hasta la fecha no se ha encontrado mucha más información de nuevas versiones o actualizaciones; resulta así de poco alcance para crear proyectos de simulación que incluyan componentes y protocolos recientes.	Al usar un lenguaje de programación para diseñar y configurar los parámetros de una red, le da mayor precisión y flexibilidad a la simulación, lo que le da escalabilidad.	Al ser un software creado bajo la tutela de Cisco, lo hace estar actualizado en varios aspectos de las redes de datos, no en todos.
Documentación	Se encuentra buena documentación en la página oficial, conteniendo ligas que ayudan a extender el conocimiento del software y de todos sus componentes.	En general hay buena documentación, desde cómo funciona el código fuente hasta las demás librerías que necesita para su correcta ejecución y poder utilizar el editor gráfico.	La documentación que se encuentra en la red es buena y suficiente para poder usar este software de manera correcta y sacarle el máximo provecho.
Estabilidad	Buena con una simulación que contenga menos de 8 dispositivos, con más elementos el simulador muchas veces se congela y marca varios errores de compilación.	Si la compilación se realiza correctamente, el editor gráfico muestra los resultados obtenidos de forma íntegra y clara, haciéndolo muy estable.	Muy estable y confiable, si se cuenta con recursos del sistema apropiados se pueden simular complejas topologías de red sin ningún problema.

Capítulo 4. GNS3

4.1 Introducción

La necesidad de los diseñadores, administradores y estudiantes de las redes de datos de tener un ambiente de simulación lo más apegado a la realidad posible, ha llevado a los desarrolladores de los simuladores a crear softwares cada vez más apegados a la realidad y con un amplio rango para realizar pruebas.

Se presenta en el capítulo cuatro el simulador central de este estudio, un software que cuenta con muchas de las características que los estudiosos de las redes de datos buscan en un simulador y que a continuación se presentan.

4.2 Características y requerimientos

GNS3 es un simulador gráfico de redes que permite diseñar fácilmente topologías de red y luego ejecutar simulaciones en las mismas.
Desarrollado inicialmente por Jeremy Grossmann, más tarde se involucraron otros desarrolladores como David Ruiz, Romain Lamaison, Aurélien Levesque y Xavier Alt.
Se ejecuta sobre Dynamips (programa básico que permite la emulación de imágenes de sistemas operativos de ruteadores y switches) para crear un entorno gráfico, haciéndolo más amigable de usar [31].

Una de las principales ventajas que tiene GNS3 es que es libre, con lo que cualquier usuario puede adquirirlo de forma gratuita, sin inscribirse a ningún sitio, y acceder al código fuente del mismo para modificarlo si así lo desea. También se puede usar en los sistemas operativos Windows, Mac OS X y Linux, así como emular plataformas de ruteadores de varios fabricantes, por lo que este software está adquiriendo popularidad en el ambiente de los diseñadores y gestores de redes de datos.

Otra ventaja es que un usuario puede extender la topología virtual creada en el simulador, conectando la interfaz física de red de su propio equipo de cómputo o conectar una máquina virtual que emule un sistema operativo, ampliando así la variedad de pruebas a realizar.
También es posible efectuar una captura de paquetes que pasan a través de una red creada en el simulador, con el software Wireshark, y simular algunas características de IPv6 que en Packet Tracer no es posible.
Permite a su vez realizar túneles para poder pasar a través de una red que solo maneja IPv4, desde dos redes origen y destino que solo soporten IPv6.

GNS3 también es compatible con otros programas de emulación como **Qemu** (emulador de procesadores que tiene capacidades de virtualización dentro de un sistema operativo), **Pemu** (emulador de Cisco PIX firewall basado en Qemu) y **VirtualBox** (software de virtualización para arquitecturas x86). Estos programas se utilizan para emular sistemas operativos de ruteadores como el IOS de Cisco, JunOS de Juniper, switches ATM, Frame Relay, Ethernet, IDS y PIX firewalls.

A pesas de que GNS3 es libre y de código abierto, debido a restricciones de licencia, el usuario tiene que adquirir los sistemas operativos de algunos dispositivos que desee usar en el simulador, por ejemplo, los IOS de Cisco.
Un ruteador en un entorno virtual en GNS3 proporciona un rendimiento alrededor de 1.000 paquetes por segundo, en cambio un ruteador normal (real) proporciona de cien a mil veces mayor rendimiento. Por lo anterior, se puede notar que este software no pretende tomar el lugar de un ruteador real, sino solo ser una herramienta para el aprendizaje y poder realizar pruebas en un entorno de laboratorio.

Dynamips

Es un emulador de IOS de equipos Cisco, que emula a las plataformas 1700, 2600, 3600, 3700 y 7200.

Este emulador se utiliza como plataforma de entrenamiento al emplear software del mundo real en un ambiente simulado, y permitir familiarizarse con dispositivos de algunas marcas conocidas, ayudando así a experimentar las funciones de ruteadores y switches.
Se pueden también probar configuraciones que rápidamente podrían ser implementadas en ruteadores en un ambiente de producción real.
Dynamips utiliza las herramientas de Ghostios, Sparsemem y Mmap para optimizar el uso de memoria, tanto real como virtual, del host emulador [32].

Dynagen

Es un software de interacción con el usuario basado en texto, escrito por Greg Anuzellique. Interactúa con Dynamips permitiendo a los usuarios listar los dispositivos, suspenderlos y recargarlos; determinar y administrar los valores de Idle-PC; realizar capturas, etc [33] (ver figura 14).

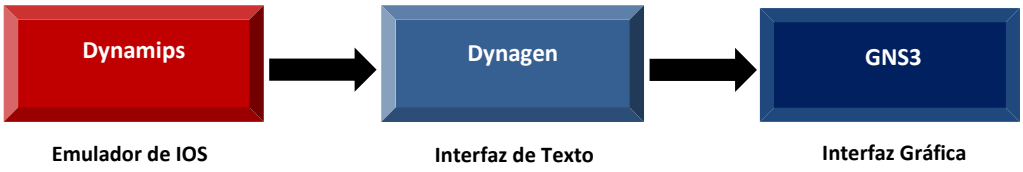


Figura 14. Arquitectura de GNS3.

Requerimientos

Las características que debe tener un equipo de cómputo para poder instalar y usar el simulador de redes GNS3 de una forma óptima, varían de acuerdo al tipo de topologías que se quieran simular. Para topologías de red que no sean muy complejas, donde se utilice un número no mayor a 10 ruteadores por simulación y donde los mismos no demanden un número mayor de recursos, las siguientes características serán suficientes:

- 2 GB de RAM
- 1 procesador de doble núcleo
- 100 MB disponibles en disco duro

Tabla 7. Comparación de los simuladores estudiados

Simulador	Soporte IPv6	Sistema operativo	Protocolos de ruteo	RAM minima requerida	Espacio en disco	Tipo licencia
NEST	No	Unix	Los más básicos	256 MB	400 MB	Libre
MaRS	No	Unix y Windows	RIP, IS-IS y OSPF	512 MB	400 MB	Libre
SSF	No	Linux y Windows	RIP, OSPF, IGRP, IS-IS y BGP	512 MB	300 MB	Libre y propietario
J-Sim	No	Multiplataforma	RIP, OSPFv2, DVMRP, MOSPF y CBT.	256 MB	200 MB	Libre
ns-2	No	Linux, Mac OS y Windows	RIP, IS-IS y OSPF	256 MB	320 MB	Libre
Real	No	Linux	RIP, IS-IS y OSPF	512 MB	300 MB	Libre y propietario
NCTUns 2.0	No	Windows y Linux	RIP, OSPF y EIGRP	256 MB	400 MB	Propietario
Packet Tracer	Si	Linux y Windows	RIP, EIGRP y OSPF	256 MB	400 MB	Propietario
OPNET IT Guru Academic	No	Windows	BGP,EIGRP, IGMP, IS-IS, IGRP, OSPF, RIP.	256 MB	400 MB	Libre
OPNET Modeler	Si	Windows	BGP,EIGRP, IGMP, IS-IS, IGRP, OSPF, RIP, MPLS y OSPFv3.	512 MB	600 MB	Propietario
GNS3	Si	Linux, Windows y Mac OS	IGRP, OSPF, RIP, RIPng, BGP, OSPF y OSPFv3.	512 MB	100 MB	Libre

Capítulo 5. Breve revisión de los protocolos de ruteo

5.1 Introducción

Los protocolos de ruteo son los encargados de hacer que los paquetes de información enviados por un emisor lleguen de manera completa, correcta y eficientemente al receptor. Esto lo hacen por medio de un conjunto de reglas que son utilizadas por un ruteador o switch de capa 3, cuando se comunica con otros ruteadores, con el fin de compartir información de enrutamiento; dicha información se usa para construir y mantener las tablas de enrutamiento [34].

Se presentan los tipos de protocolos de ruteo y el tipo de enrutamiento que utilizan, así como los utilizados por IPv6.

5.2 Características de los protocolos de ruteo

Tipos de Enrutamiento

Los protocolos de enrutamiento usan mecanismos distintos para crear las tablas de enrutamiento de los ruteadores, así como para determinar cuál será la mejor ruta para llegar a cualquier host remoto. Existen tres tipos de enrutamiento y son los siguientes:

Enrutamiento Estático. En este tipo de enrutamiento se introducen de forma manual en los ruteadores toda la información que contienen los mismos. El principal problema que presenta es que todos los cambios que pudiera haber en las rutas de la red deberán actualizarse de forma manual por un administrador de la red.

La ventaja de este método, además de la simpleza para configurarlo, es que no supone ninguna sobrecarga adicional de trabajo sobre los ruteadores y los enlaces en una red pequeña.

Enrutamiento Predeterminado. Es una ruta estática que se establece por antelación como una conexión de salida o Gateway por donde saldrán todos los paquetes que tengan una IP

desconocida por el ruteador. Es la forma más fácil de enrutamiento para un ruteador conectado a un único punto de salida. Esta ruta se indica en IPv4 como la red **0.0.0.0/0.0.0.0**.

Enrutamiento Dinámico. Las tablas de enrutamiento se mantienen actualizadas de forma dinámica por medio de mensajes de actualización, enviados por los protocolos de ruteo, indicando al software del ruteador que actualice la tabla de enrutamiento en consecuencia.

IGP (Interior Gateway Protocols)
Se encargan del enrutamiento de paquetes dentro de un dominio de enrutamiento o sistema autónomo.

EGP (Exterior Gateway Protocols)
Se usan para que pueda haber intercambio de información de ruteo entre los distintos sistemas autónomos que hay, proporcionando una vista más estructurada de Internet mediante la división de dominios de enrutamiento.

Algunos protocolos de enrutamiento más comúnmente utilizados en IPv6 se describen a continuación.

RIPng o RIPv6.- Es un protocolo de encaminamiento dinámico de tipo IGP (Internal Gateway Protocol), mediante el cual los ruteadores pertenecientes a un mismo Sistema Autónomo (AS) intercambian y actualizan sus correspondientes tablas de rutas. Constituye la versión de RIP disponible para IPv6 [35].

OSPFv3.- Es la versión de OSPF para IPv6 que está basada en OSPFv2, contiene varias adiciones para poder distribuir prefijos de IPv6 y utilizarlo como transporte. También es de tipo IGP.

EIGRPv6.- Es una versión mejorada del IGRP desarrollada por Cisco. Es un protocolo de vector distancia mejorado que se basa en el algoritmo de actualización difusa (DUAL, por sus siglas en inglés) para calcular la ruta más corta a un destino dentro de una red.

IS-IS para IPv6.- Es un protocolo de enrutamiento interior y de estado de enlace que está pensado para soportar enrutamiento en grandes dominios. Permite a sistemas intermedios

(IS's) dentro de un mismo dominio, cambiar su configuración e información de ruteo para facilitar la información de encaminamiento y funciones de transmisión de la capa de red. Las características de IPv6 para IS-IS permiten que se sumen a las rutas IPv4 los prefijos IPv6, creando un nuevo "address family" para incluir IPv6. IS-IS IPv6 soporta tanto "single-topology" como "multiple-topology" [36].

BGP4+.-. Se trata de una actualización de BGP4 que soporta entre otras funcionalidades, IPv6. Permite el encaminamiento de los paquetes IP que se intercambian entre distintos AS mediante el intercambio de forma dinámica de prefijos de rutas, lo cual se lleva a cabo mediante el establecimiento de sesiones BGP inter-AS sobre conexiones TCP. Este tipo de operación proporciona comunicación fiable y esconde todos los detalles de la red por la que se pasa [37].

Capítulo 6. Prácticas propuestas y preparadas

6.1 Introducción

En este capítulo se presentan resumidamente, las prácticas desarrolladas y algunas implementadas, a dos grupos de alumnos, con el soporte de IPv6 en mente. Estas prácticas incluyeron los siguientes temas:

- Instalación y configuración de GNS3
- Ruteo estático con IPv4 e IPv6 en GNS3
- RIP en GNS3
- RIPng en GNS3
- Autoconfiguración Stateless en GNS3
- BGP en GNS3
- Túnel con Autoconfiguración y ruteo estático en GNS3
- Túnel con Autoconfiguración, RIPng y RIP en GNS3
- Túnel con Autoconfiguración y BGP en GNS3

Práctica #1:

6.2 Instalación y configuración de GNS3

Elaboración: Junio 2013
Última Revisión: Febrero 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo de realización: 1 hora con 20 minutos.

Objetivo

Conocer como instalar y configurar el software GNS3, así como aprender el funcionamiento y las características con las que cuenta mediante la creación de una topología de red, que servirá de base para las siguientes prácticas.

Desarrollo

Instalación de GNS3

Descargar el programa GNS3 de su página oficial que es: **http://www.gns3.net/download** y seleccionar para el sistema operativo Windows la versión **GNS3 all-in-one** (ver figura 1), ya que esta incluye Dynamips, Putty (cliente dinámico para conexiones SSH y Telnet), WinPCAP (conjunto de librerías para trabajar con protocolos de red presentes en los analizadores de redes), vpcs (permite simular PC virtuales en una topología de red creada con Gns3), Wireshark y otras herramientas necesarias para ampliar el rango de pruebas.

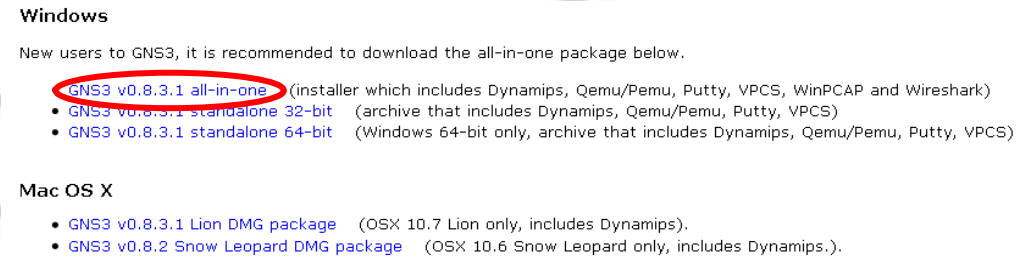


Figura 1. Ubicación de la liga de descarga de GNS3 en su página oficial.

Una vez que ya se descargó el programa se tendrá que ejecutar el mismo, aparecerá un asistente de instalación donde solo se tendrá que dar clic en siguiente para que se instalen los programas y herramientas necesarios para el buen funcionamiento del simulador, y para tener amplias opciones a la hora de realizar las pruebas.

Al abrir GNS3 por primera vez se abrirá un asistente de configuración (ver figura 2). Para esta práctica no se hará uso del mismo por lo que se deberá cerrar la ventana del **Wizard**.

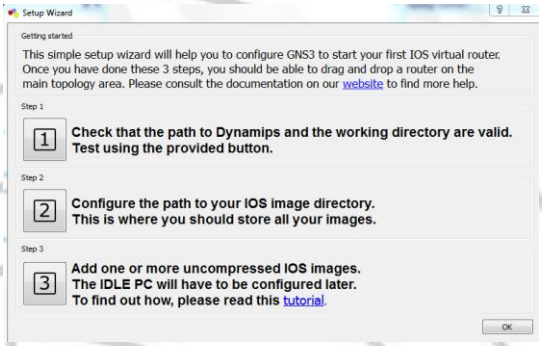


Figura 2. Ventana del asistente de configuración de GNS3.

Instalación de Imágenes IOS

> **Nota:** Los ruteadores seleccionados para esta práctica son del modelo Cisco© 2600, cuya imagen del sistema operativo (IOS) no vienen incluidas previamente en el software GNS3, por lo que deberá solicitar las mismas al instructor. Su uso es para fines académicos y únicamente podrá utilizarse para esta práctica.

Lo primero que se hará será cambiar el idioma del programa al español ya que por defecto viene en inglés, esto además de cambiar el lenguaje del programa, creará una carpeta de trabajo llamada **GNS3** en el directorio del usuario, ahí es donde se guardarán los proyectos y las imágenes de los IOS que se utilizarán. Para realizar lo anterior, ir al menú **Edit** > **Preferences**, se abrirá una ventana donde al desplegar el submenú en el recuadro **Language** se podrá cambiar el idioma (ver figura 3).

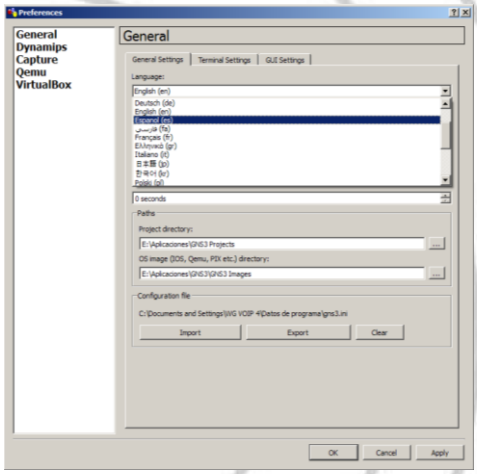


Figura 3. Ventana donde se podrá cambiar el idioma del programa.

Enseguida se tendrán que descargar las imágenes IOS o conseguirlas con el instructor para hacer uso de los ruteadores de Cisco en el área de trabajo del programa, ya que estas imágenes permiten activar los ruteadores virtuales. Para crear la topología que se usará en esta práctica, se manejará un solo modelo de ruteador por lo que se utilizará la imagen de su sistema operativo (ver figura 4).

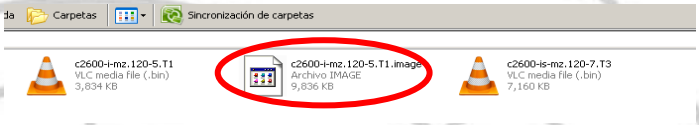


Figura 4. Archivo imagen IOS del ruteador c2600.

Una vez conseguida la imagen, ubicarla en la carpeta llamada **Images** que se encuentra en la carpeta de trabajo que se creó anteriormente al realizar el cambio del idioma (ver figura 5).

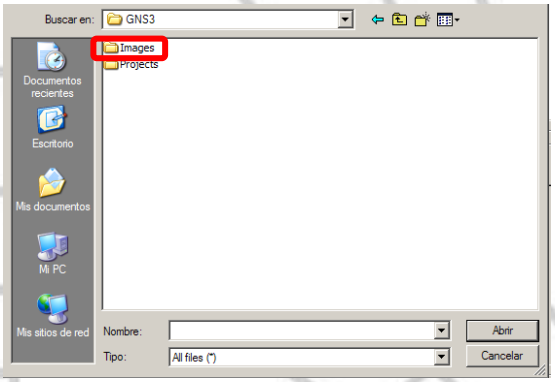


Figura 5. Ubicación de imágenes IOS de los ruteadores.

Posteriormente, seleccionar el IOS desde el menú **Editar** y escoger la opción que dice: ***Imagenes IOS y hypervisors***.

En la parte donde dice **Archivo de Imágenes** seleccionar un IOS de los que se descargaron y que se usará (ver figura 6). Si la imagen está comprimida aparecerá un mensaje indicando si se quiere descomprimir dicha imagen, decir que si se desea hacerlo.

Se pueden personalizar algunos datos más, en caso de ser necesario o dejar los valores por defecto de los parámetros siguientes:

- El modelo donde se aplicará el IOS,
- La memoria RAM que usará,
- Y el IDLE PC

Después de agregar una imagen dar clic en el botón **Guardar**. Si se desea agregar otra imagen volver a seleccionarla en **Archivo de Imágenes** y volver a guardarla, esto irá agregando las imágenes en la ventana superior. Por último dar clic en el botón **Cerrar**.

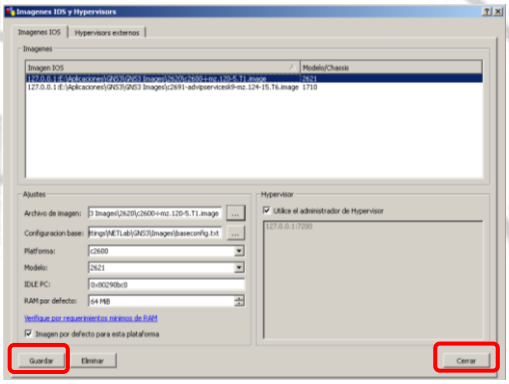


Figura 6. Ventana **Imagenes IOS y hypervisors** donde se agregan las imágenes IOS.

Configuración de Dynamips

En el menú **Editar > Preferencias** escoger la opción **Dynamips**, verificar que está indicada la ruta donde se encuentra el ejecutable de Dynamips. También verificar que las siguientes opciones estén seleccionadas:

- "Habilitar la función de ghost IOS" para utilizar la función ghost de Dynamips en forma global, ya que reduce significativamente el uso de memoria RAM real necesario para los equipos que corren con la misma imagen de IOS.
- "Habilitar la función de nmap" para utilizar la función nmap de Dynamips en forma global, ya que esto disminuirá la cantidad de memoria RAM que toman las imágenes IOS del sistema.
- "Habilitar la función de esparcir memoria" para utilizar la función "sparsemem" de Dynamips en forma global, para reducir la cantidad de memoria virtual utilizada por las instancias de los ruteadores.

Después probar el módulo Dynamips dando clic al botón **Test Settings**. Deberá salir un mensaje en verde diciendo que Dynamips se inició con éxito (ver figura 7). En caso afirmativo ya se podrá empezar a usar Dynamips junto con GNS3.

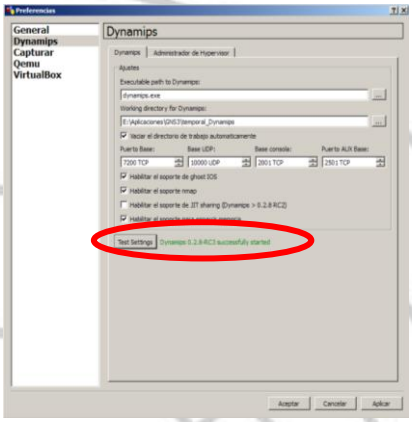


Figura 7. Ventana de configuración y verificación de Dynamips.

Configuración de las Computadoras Virtuales

Para poder trabajar con una imagen de una computadora en el área de trabajo de GNS3, se deberán realizar primero los siguientes pasos:

- Ir a la carpeta donde se instaló GNS3 y buscar el archivo **cygwin1.dll**, copiar el mismo y pegarlo dentro de la carpeta **vpcs** que se encuentra dentro de la misma carpeta de GNS3.
- Abrir la carpeta **vpcs**. Vpcs es una aplicación diseñada para dynamips que permite simular hasta 9 computadoras y ejecutar algunos comandos como **ping** o **trace** en las PC. Cuando VPCS inicia empieza a escuchar en los puertos desde el 20000 al 20008.
- Dar doble clic al archivo **vpcs.exe**, se abrirá una terminal de Windows.
- Configurar una PC. Cuando se abra la terminal por defecto se estará en la configuración de la PC número 1, esto se puede comprobar porque en el prompt aparecerá entre corchetes el número de la máquina, ejemplo: **VPCS[1]>**
- Asignar una IP a esta máquina, su Gateway por defecto y su máscara de red (expresada por el número de bits). Por ejemplo: **ip 192.168.1.1** 192.168.1.254 **24**
- Se tendrá que realizar lo mismo para cada equipo que se deseé agregar, por ejemplo para la PC 2 se tecleará el número 2 para cambiar el prompt a **VPCS [2]>** y agregarle los valores del paso anterior (ver figura 8).

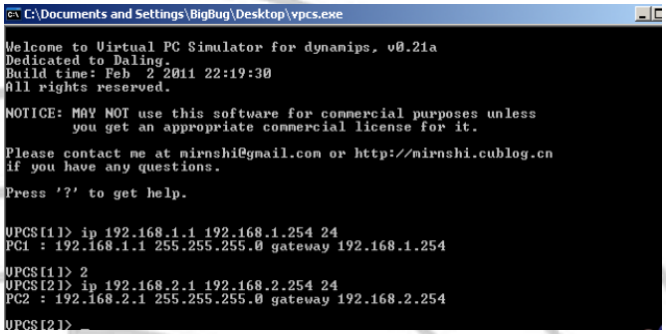


Figura 8. Ventana de la terminal de VPCS que funciona como la terminal de las PC virtuales de GNS3.

Para integrar vpcs dentro de GNS3, se tendrá que seleccionar del menú **Editar**, **Symbol Manager,** y en la parte que dice **símbolos disponibles** seleccionar el símbolo de una computadora, después dar clic en el botón que tiene la flecha apuntando hacia la derecha, que se encuentra en medio de la ventana, para agregar dicho icono (ver figura 9).

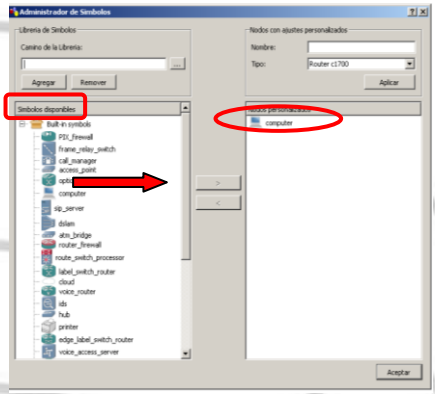


Figura 9. Ventana de configuración de los símbolos de GNS3.

En la parte superior derecha donde dice **nodos con ajustes personalizados** poner el nombre del nodo (el que se desee), y en donde dice **tipo**, escoger la opción de **nube**, dar clic en **Aplicar** y por último en **Aceptar** (ver figura 10).

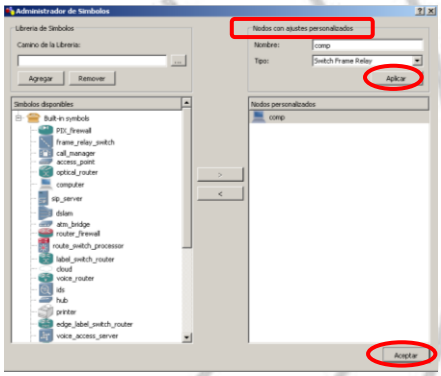


Figura 10. Asignación del nombre y el tipo al símbolo que se agrega.

Creación de una Topología de Red

1.- Agregar el símbolo de la PC configurada en el paso anterior, este símbolo aparece en la columna izquierda de la ventana principal, arrastrándolo al área de trabajo del lado derecho de la pantalla. Para esta práctica se usarán dos PC por lo que se añadirán dos símbolos de PC al área de trabajo (ver figura 11).

Figura 11. Adición de las PC virtuales al área de trabajo de GNS3

2.- Para configurar cada PC se tendrá que dar clic derecho sobre su imagen y seleccionar la opción **Configurar** (ver figura 12).

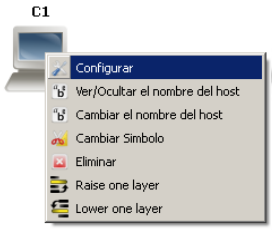


Figura 12. Menú donde se abre la ventana de configuración de la PC virtual.

3.- Dar clic en **C1,** que aparece del lado izquierdo de la ventana emergente, después en la pestaña que dice **NIO UDP** y ahí, en dado caso de que no se encuentren interfaces ya agregadas a la ventana de **NIOs**, añadir las mismas agregando el puerto remoto y local, así como el host remoto, con el botón que dice **Agregar**. Por default estos valores inician con 30000 para el puerto local y con 20000 para el puerto remoto, el host remoto viene con la dirección 127.0.0.1. Por último dar clic en **Aceptar** (ver figura 13).

Para la segunda PC se deberá sumar una unidad al valor del puerto local y remoto, se tendrá que ir sumando el valor de uno por cada PC que se agregue a la topología.

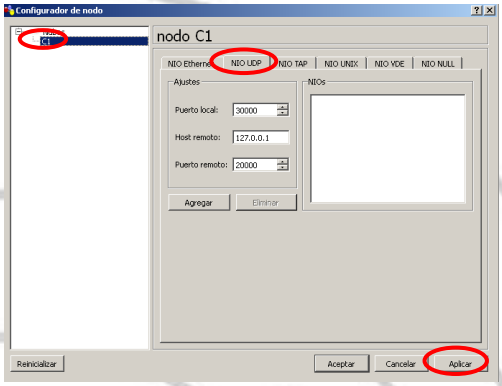


Figura 13. Ventana donde se agrega el puerto local y remoto, así como la dirección del host remoto a la PC.

4.- Después agregar los ruteadores al área de trabajo de GNS3 por medio del arrastre de sus imágenes con el ratón desde la ventana ubicada a la izquierda de la ventana principal. Cabe señalar que solo se podrán elegir los símbolos de los modelos cuyas imágenes del IOS, se agregaron con anterioridad (sección Instalación de Imágenes IOS). En este ejemplo se seleccionaron dos ruteadores del modelo c2600 (ver figura 14).

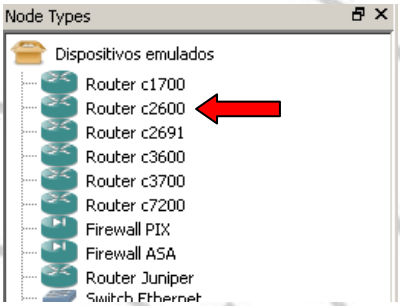


Figura 14. Menú de los dispositivos emulados.

5.- Ahora se procederá a realizar las conexiones entre los equipos con la opción de **Agregar un Vínculo,** ubicada en la parte superior de la ventana principal. Al darle clic se abrirá un submenú donde se elegirá el tipo de conexión que se va a utilizar para unir a los dispositivos, esto se hará para todos los equipos que conforman la topología de tal forma, que estos queden interconectados entre sí (ver figuras 15 y 16).

Nota: Para la conexión entre los ruteadores se utilizará un conector de tipo **Serial** y para conectar los ruteadores con las PC se hará con un conector de tipo **FastEthernet.**

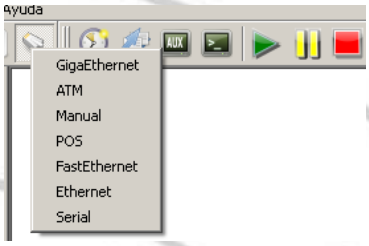


Figura 15. Submenú donde se agregan el tipo de conexión que conectará a los dispositivos de la topología.

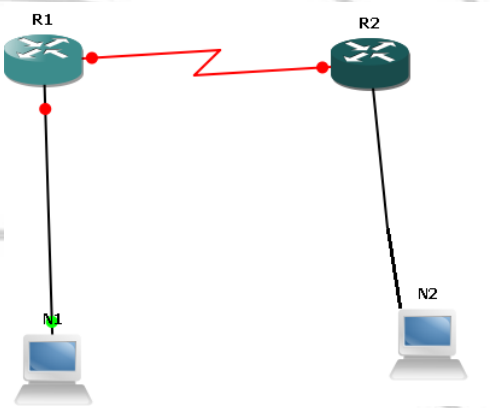


Figura 16. Dispositivos ya conectados entre sí con los medios de conexión agregados en el paso anterior.

6.- Para identificar de forma visual los segmentos de red que tiene cada subred, conviene agregar una nota desde el icono que se encuentra en la barra de herramientas superior de la ventana principal (ver figura 17), y así agregar la IP de cada interfaz (de acuerdo a las prácticas siguientes) en la maqueta, al lado de cada equipo.

Figura 17. Adición de una nota a la topología de red.

Topología Final

La topología deberá quedar de la siguiente forma:

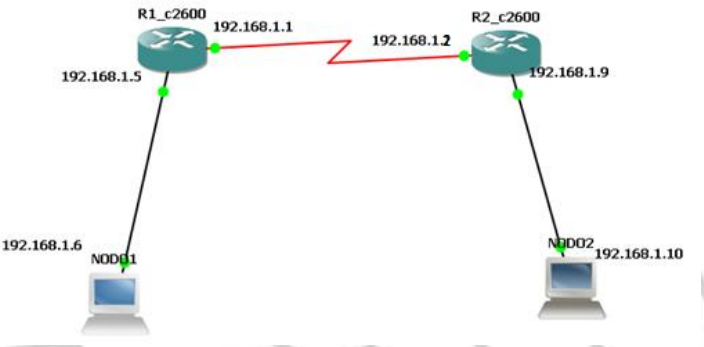


Figura 18. Ejemplo de Topología de red final.

Copiar una imagen de la topología creada por usted y pegarla en la siguiente tabla:

Resultado Final

Práctica #2

6.3 Ruteo estático con IPv4 e IPv6 en GNS3

Elaboración: Julio 2013
Última Revisión: Febrero 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo de realización: 1 hora.

Objetivo

Conocer el funcionamiento del ruteo estático con IPv4 e IPv6 y la forma de poder realizar su implementación en el software de simulación de redes GNS3, mediante la configuración de una ruta predeterminada.

Desarrollo

Creación de una Topología de Red

Crear una topología con dos PC y dos ruteadores de la serie c2600 (ver figurar 1).

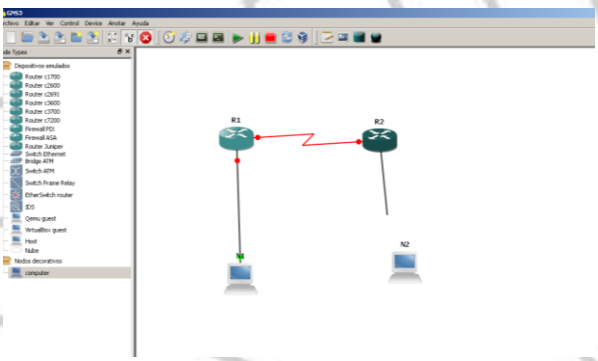


Figura 1. Dispositivos ya conectados entre sí con los medios de conexión.

Configuración de los ruteadores

Para configurar los ruteadores habrá que posicionarse con el ratón sobre cada uno, dar clic derecho y escoger la opción **Iniciar**, esto activará al ruteador (ver figura 2).

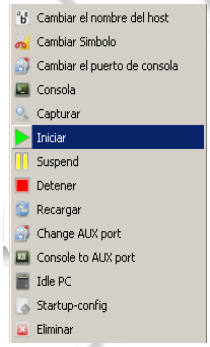


Figura 2. Ventana para inicia al ruteador.

Después volverle a dar clic derecho sobre el ruteador y seleccionar la opción **Idle PC,** se abrirá una pantalla en donde se listan los valores potenciales del mismo. Se debe escoger el valor que reduzca más el consumo de la memoria de la PC, por lo general estos valores están marcados con un asterisco (ver figuras 3 y 4).

Esto es para darles una correcta asignación de memoria a los equipos, ya que en su afán de imitar a un equipo real, GNS3 asigna recursos de la memoria a los ruteadores virtuales.

El comando **Idle PC** efectúa un análisis en la imagen que se está ejecutando para determinar cuáles son los posibles puntos en el código que representan un bucle de **Idle** en el IOS. Una vez aplicado, **Dynamips** "duerme" ocasionalmente al ruteador virtual cuando el bucle **Idle** es ejecutado, reduciendo significativamente el consumo de CPU del host, sin reducir la capacidad del ruteador virtual de realizar sus tareas.

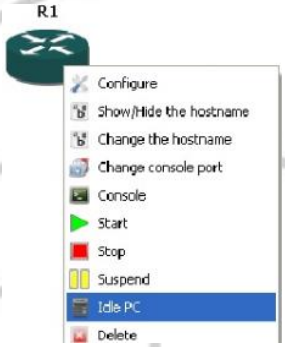


Figura 3. Menú donde se inicia **Idle PC**.

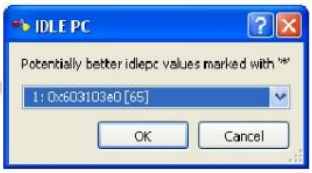


Figura 4. Selección del valor de **Idle PC**.

Abrir una terminal del ruteador dando clic con botón derecho del ratón sobre la imagen del mismo y seleccionar **Consola** (ver figura 5). Cuando se presente la opción de diálogo de configuración, responder que "no" (ver figura 6).

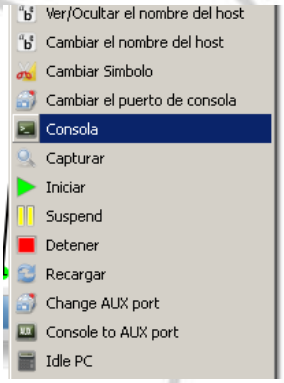


Figura 5. Menú donde se abre la terminal del ruteador.

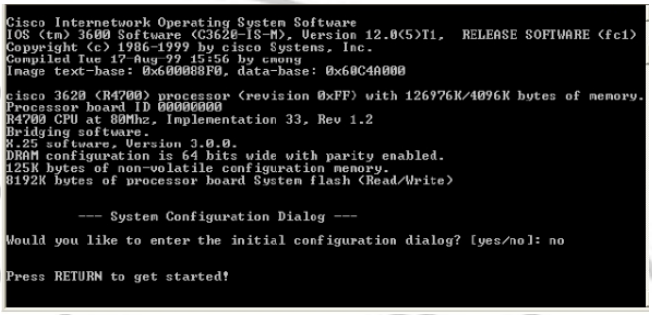


Figura 6. Ventana que se muestra al iniciar la terminal del ruteador.

.

En la terminal del ruteador 1 teclear los siguientes comandos que aparecen en la tabla 1 para configurar la interfaz serial, agregándole una dirección IPv4 (ver figura 7):

Tabla 1. Comandos de configuración de interfaces.

enable
config terminal
int s0/0
ip add 192.168.1.1 255.255.255.0
no shutdown

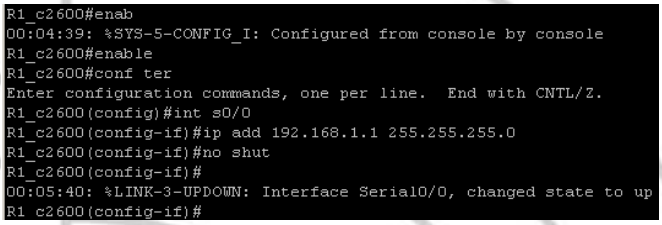


Figura 7. Configuración de la interfaz serial en la terminal del ruteador 1.

Hacer lo mismo con la interfaz f0/0 del ruteador 1 (ver figura 8).

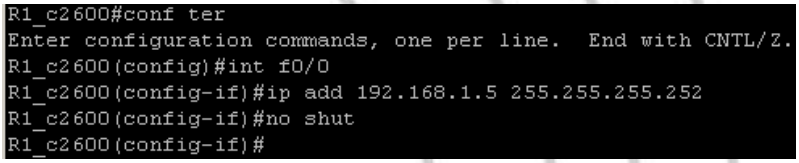


Figura 8. Configuración de la interfaz FastEthernet en la terminal del ruteador 1.

En el ruteador 1, se debe configurar la ruta por defecto, para esto se deberá teclear en la terminal el comando: **ip route 0.0.0.0 0.0.0.0** (ver figura 9).

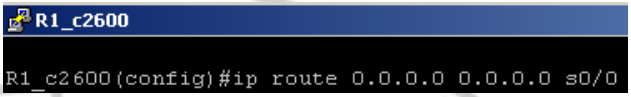


Figura 9. Configuración de la ruta por defecto en la terminal del ruteador 1.

Topología Final

La topología finalmente deberá quedar de la siguiente forma:

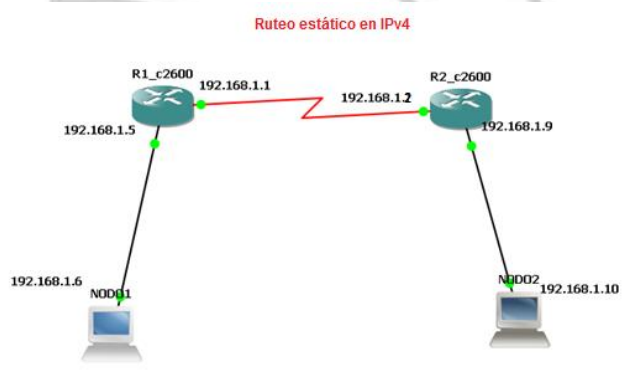


Figura 10. Topología final.

¿Con qué comando se pueden ver todas las rutas IPv4 que tiene configuradas el ruteador 1?

Teclear dicho comando y poner los resultados obtenidos en la siguiente tabla:

¿Con qué comando se pueden ver las interfaces que tiene asignadas el ruteador 1?

Teclear dicho comando y poner los resultados obtenidos en la siguiente tabla:

Repetir los mismos pasos que se realizaron para la configuración de las interfaces y la ruta por defecto del ruteador 1 pero ahora realizarlo para el ruteador 2 y poner los resultados obtenidos en la siguiente tabla:

Interfaces:
Ruta por defecto:

Se puede verificar que todos los equipos están comunicados haciendo "pings" entre los mismos en la terminal de los ruteadores.

Poner los resultados obtenidos en la siguiente tabla:

¿Con qué comando se puede trazar la ruta que siguen los paquetes de comunicación entre los equipos de la topología realizada?

Poner los resultados obtenidos con dicho comando en la siguiente tabla:

Se realizarán los mismos pasos que se hicieron anteriormente para configurar el ruteo estático pero ahora con IPv6.

a) Para esto se deberá crear una topología con dos PC y dos ruteadores de la serie c2691.

Para que se puedan realizar conexiones con cables de tipo serial en el ruteador de este modelo, se deberá dar clic derecho sobre la imagen del mismo y escoger la opción **Configurar;** se abrirá una ventana en la cual se debe dar clic izquierdo en **R1** (dependiendo del ruteador en el que se esté)**,** después en la pestaña **Slots** y en la parte de WICs seleccionar **wic 0:** escoger del submenú la opción **WIC-1T** (ver figura 11). Finalmente dar clic en **Aceptar**.

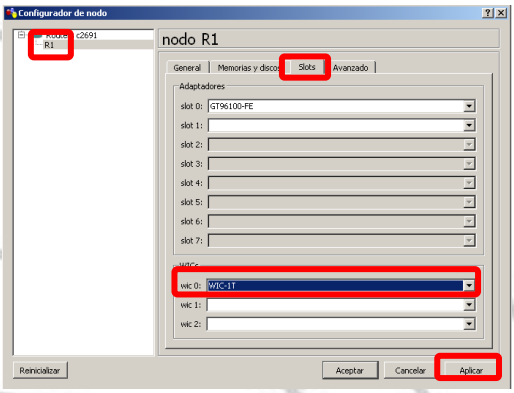


Figura 11. Ventana de configuración inicial del ruteador 1.

La topología deberá quedar como se muestra en la siguiente figura 12:

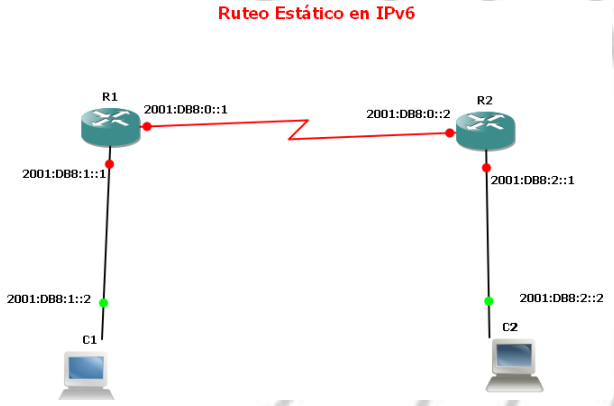


Figura 12. Topología final con IPv6.

Nota: Los ruteadores seleccionados para esta práctica son del modelo Cisco© 2691, cuya imagen del sistema operativo (IOS) no viene incluida previamente en el software GNS3, por lo que deberá solicitar la misma al instructor. Su uso es para fines académicos y únicamente podrá utilizarse para esta práctica.

b) En la terminal del ruteador 1 teclear los siguientes comandos para configurar la interfaz serial agregándole una dirección IPv6 (ver tabla 2):

Tabla 2. Comandos de configuración de la interfaz serial en la terminal del ruteador 1.

R1> enable R1# configure terminal R1 (config-if)#interface Serial 0/0 R1 (config-if)# ipv6 address (dirección IPv6)/64 R1 (config-if)# no shutdown

c) Hacer lo mismo con la interfaz FastEthernet del ruteador 1 (ver tabla 3).

Tabla 3. Comandos de configuración de la interfaz FastEthernet en la terminal del ruteador 1.

R1 (config)#interface FastEthernet 0/0 R1 (config-if)# ipv6 address (dirección IPv6)/64 R1 (config-if)# no shutdown

d) En el ruteador 1, también se debe configurar la ruta estática por defecto, para esto se tendrá que teclear en la terminal del mismo, en el modo configuración, los comandos siguientes:

Tabla 4.3. Comandos de configuración de la ruta estática por defecto en el ruteador 1

R1 (config)# ipv6 unicast-routing R1 (config)# ipv6 route ::/0 s0/0.

.

e) Repetir los incisos b), c) y d) para el ruteador 2 y poner los resultados obtenidos en la siguiente tabla:

b)
c)
d)

f) Dar doble clic al archivo **vpcs.exe**, se abrirá una terminal de Windows que por defecto estará en la configuración de la PC número 1.

g) Asignar una IP a esta máquina, su Gateway por defecto y su máscara de red (expresada por el número de bits). Por ejemplo: **ip 2001:db8: 1::2** 2001:db8: 1::1 **64.** (ver figura 13).

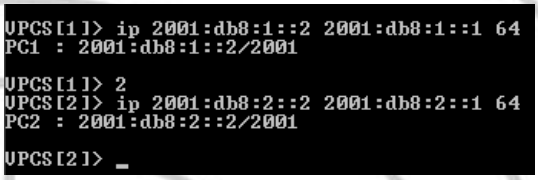


Figura 13. Asignación de las direcciones de las PC en la terminal de VPCS.

Teclear el comando con el que se pueden ver las rutas IPv6 que tienen configuradas los ruteadores y poner los resultados obtenidos en la siguiente tabla:

R1
R2

Poner las interfaces que aparecen en la terminal de configuración de los ruteadores en la siguiente tabla:

R1
R2

Hacer un ping desde la terminal de la PC 1 hacia la PC 2 y de la terminal del ruteador 1 hacia la PC 2, también de la terminal del ruteador 2 hacia la PC 1.

Poner los resultados obtenidos en la siguiente tabla:

PC1
R1
R2

Teclear el comando **trace** desde la terminal de la PC 1 hacia la PC 2 y de la PC 2 hacia la PC 1 y poner los resultados obtenidos en la siguiente tabla:

PC1
PC2

¿Explique por qué el comando de ruteo estático se configuró solo para la interfaz serial de los ruteadores?

_____

Práctica #3:

6.4 RIP en GNS3

Elaboración: Julio 2013
Última Revisión: Febrero 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo de realización: 40 minutos.

Objetivo

Conocer el funcionamiento y la utilización de RIP en el software de simulación de redes GNS3, para el intercambio de información de ruteo en una red local bajo una misma administración.

Desarrollo

Nota: Se deberá haber descargado previamente el software GNS3 de su página oficial, tenerlo instalado, y configurado con los emuladores y librerías que se incluyen en su carpeta de instalación. Además agregarle una imagen IOS de Cisco del ruteador a usar en esta práctica y configurar los iconos de las PC en el submenú de administrador de símbolos, que se encuentra en el menú **Editar**, para que se pueda comunicar con el software **vpcs**.

Los ruteadores seleccionados para esta práctica son del modelo Cisco© 2600, cuya imagen del sistema operativo (IOS) no viene incluida previamente en el software GNS3, por lo que deberá solicitar la misma al instructor. Su uso es para fines académicos y únicamente podrá utilizarse para esta práctica.

Creación de la Topología de Red

Crear una topología de red con dos ruteadores y dos PC. La topología deberá quedará de la siguiente forma (ver figura 1):

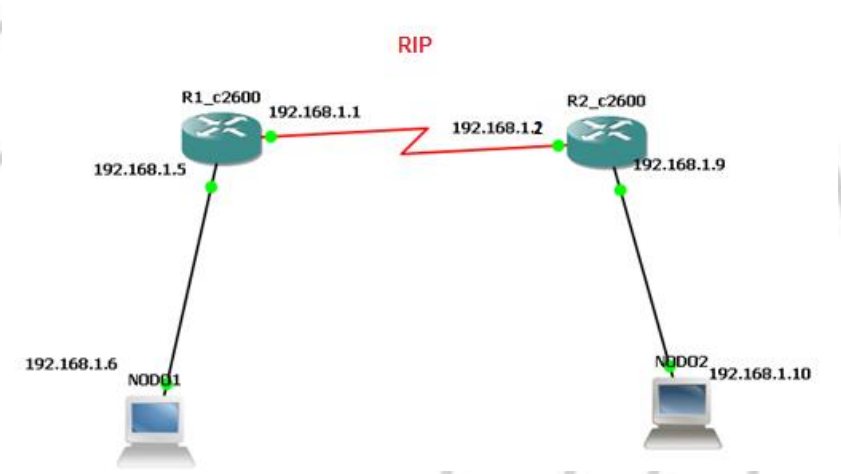


Figura 1. Ejemplo de Topología de red final.

Configuración de los ruteadores

a) Abrir una terminal del ruteador 1 y teclear los comandos que aparecen en la tabla 1 para configurar las direcciones de sus interfaces serial y FastEthernet con las direcciones IPv4 correspondientes.

Tabla 1. Comandos de configuración de las interfaces en la terminal del ruteador 1.

R1> enable R1# configure terminal R1 (config)#interface FastEthernet 0/0 R1 (config-if)# ip add **dirección IPv4** ***máscara de red*** R1 (config-if)# no shutdown R1 (config-if)#exit R1 (config)#interface Serial 0/0 R1 (config-if)# ip add **dirección IPv4** ***máscara de red*** R1 (config-if)# no shutdown

b) Para habilitar RIP, se deberán teclear los comandos que aparecen en la siguiente tabla, en la terminal del ruteador 1 (ver tabla 2).

Tabla 2. Comandos de configuración de RIP en la terminal del ruteador 1.

R1 >enable R1 #configure terminal R1 (config)# router rip **procesorip** R1 (config)# version 2 R1 (config-if)# network **IP de la red** R1 (config-if)# exit

c) Repetir los incisos a) y b) para el ruteador 2 y poner los resultados obtenidos en la terminal del ruteador en la siguiente tabla.

a)
b)

d) En la terminal de configuración de las PC asignarles su dirección IP, su Gateway por defecto y su máscara de red (expresada por el número de bits).

¿Con qué comando se puede verificar que RIP está activado en el ruteador?

_____

e) Teclear dicho comando en la terminal de los ruteadores y poner los resultados obtenidos en la siguiente tabla:

R1
R2

f) Para comprobar que hay conexión entre los dispositivos de la topología, hacer un **ping** desde la terminal de la PC 1 hacia la PC 2 y de la PC 2 a la PC 1. Poner los resultados obtenidos en la siguiente tabla:

PC1
PC2

g) Teclear el comando **trace** desde la terminal de la PC 1 hacia la IP de la PC 2 y de la PC 2 a la IP de la PC 1 para poder observar que camino siguen los paquetes que se intercambian entre las dos PC y anotar los resultados obtenidos en las siguiente tabla:

PC1
PC2

Conforme a la topología de red creada, ¿los resultados obtenidos con el comando anterior son correctos?

_____

Práctica #4:

6.5 RIPng en GNS3

Elaboración: Agosto 2013
Última Revisión: Febrero 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo de realización: 45 minutos.

Objetivo

Conocer el funcionamiento y la utilización de RIPng en el software de simulación de redes GNS3, para el intercambio de información de ruteo en una red local bajo una misma administración.

Desarrollo

Nota: Los ruteadores seleccionados para esta práctica son del modelo Cisco© 2691, cuya imagen del sistema operativo (IOS) no viene incluida previamente en el software GNS3, por lo que deberá solicitar la misma al instructor. Su uso es para fines académicos y únicamente podrá utilizarse para esta práctica.

Creación de la Topología de Red

Crear una topología de red como en la que se muestra en la siguiente figura1.

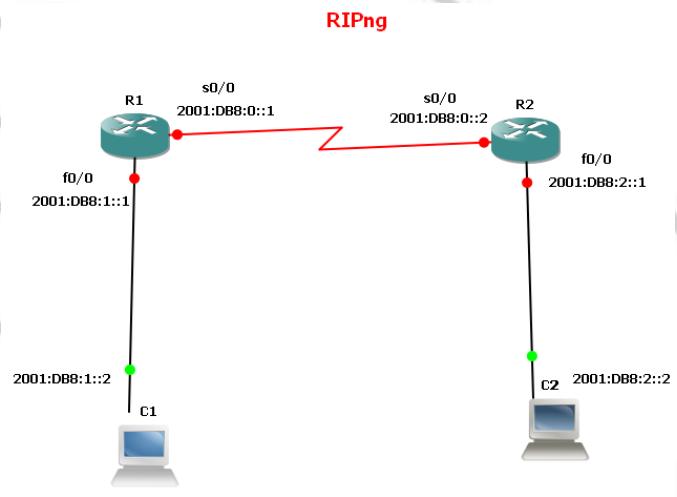


Figura 1. Ejemplo de la Topología de red a crear.

Configuración de los ruteadores

a) En la terminal del ruteador 1 teclear los comandos que aparecen en la tabla 1 para configurar las direcciones de sus interfaces serial y FastEthernet con las direcciones IPv6 correspondientes.

Tabla 1. Comandos de configuración de las interfaces en la terminal del ruteador 1.

R1> enable R1# configure terminal R1 (config)#interface FastEthernet 0/0 R1 (config-if)# ipv6 address ***(dirección IPv6)***/64 R1 (config-if)# no shutdown R1 (config-if)# exit R1 (config)#interface Serial 0/0 R1 (config-if)# ipv6 address ***(dirección IPv6)***/64 R1 (config-if)# no shutdown

b) Para habilitar RIPng, se deberán teclear los comandos que aparecen en la siguiente tabla en la terminal del ruteador 1 (ver tabla 2).

Tabla 2. Comandos de configuración de RIPng en la terminal del ruteador 1.

R1 >enable R1 #configure terminal R1 (config)# ipv6 unicast-routing R1 (config)# ipv6 router rip **procesorip** R1 (config)# interface FastEthernet 0/0 R1 (config-if)# ipv6 rip **procesorip** enable R1 (config-if)# exit R1 (config-if)#interface Serial 0/0 R1 (config-if)# ipv6 rip **procesorip** enable R1 (config-if)# exit

c) Repetir los mismos pasos para el ruteador 2 y poner los resultados obtenidos en la siguiente tabla.

a)
b)

d) Asignar una IP a las PC, su Gateway por defecto y su máscara de red (expresada por el número de bits). Por ejemplo: **ip 2001:db8:1::2** 2001:db8:1::1 **64.** (ver figura 2)

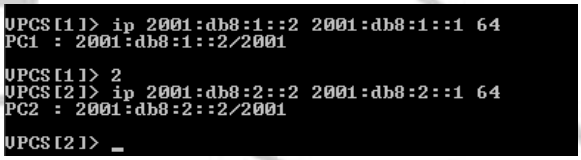


Figura 2. Ejemplo de asignación de las direcciones de las PC en la terminal de VPCS.

¿Con qué comando se puede verificar que RIPng está activado en el ruteador?

_____

e) Teclear dicho comando en la terminal de los ruteadores y poner los resultados obtenidos en la siguiente tabla:

R1
R2

f) Para comprobar que hay conexión entre los dispositivos de la topología, hacer un **ping** desde la terminal de la PC 1 hacia la PC 2 y de la PC 2 a la PC 1. Poner los resultados obtenidos en la siguiente tabla:

PC1
PC2

g) Teclear el comando **trace** desde la terminal de la PC 1 hacia la PC 2 y de la PC 2 a la PC 1 para poder observar que camino siguen los paquetes que se intercambian entre las dos PC y anotar los resultados obtenidos en las siguiente tabla:

PC1
PC2

¿Por qué no se utilizó el comando **network**, utilizado en RIP**,** en la configuración de **RIPng**?

_____

h) Ahora se analizará el tráfico que circula por la red creada desde la interfaz de un ruteador en el simulador, logrando así que la simulación se apegue aún más, a lo que sería trabajar con una red física (real).

Ir al menú **Editar** de la ventana principal de GNS3 y seleccionar la opción de **Preferencias**, se abrirá una ventana en la cual se escogerá la opción de **Capturar** (ver figura 3).

En esta ventana aparece la opción de **Directorio para los archivos de captura**, que es donde seleccionaremos el directorio y la carpeta donde queremos que se guarden todas las capturas que realicemos con el software **Wireshark**.

También seleccionar la opción **Iniciar el comando en forma automática cuando se captura** para que se abra de forma automática el programa **Wireshark** cada vez que se desee iniciar la captura de los paquetes en la red.

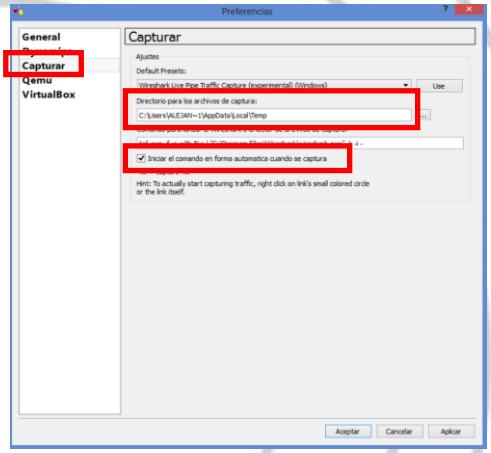


Figura 3. Ventana de las configuraciones de captura de GNS3.

i) Una vez hecho lo anterior situarse en la topología de red creada y posicionando el ratón en una interfaz de la red dar clic derecho y seleccionar la opción de **iniciar wireshark,** enseguida se abrirá una ventana preguntando en que interfaz se quiere iniciar la captura, seleccionar la interfaz deseada y dar clic en aceptar (ver figura 4).

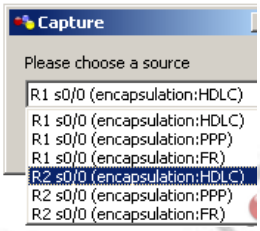


Figura 4. Ventana donde se muestran las opciones de las interfaces para capturar.

Una vez hecho lo anterior, el programa de captura de paquetes **Wireshark** comenzará a iniciar la captura del tráfico de la red que pasa por la interfaz seleccionada.

j) Observar lo que ocurre en el software **Wireshark** inmediatamente después de teclear el comando **ping** y **trace** en la terminal de cualquier ruteador. Hacer una captura de pantalla de lo que se ve en el analizador y pegar dicha imagen en la siguiente tabla:

Práctica #5:

6.6 Autoconfiguración Stateless en GNS3

Elaboración: Agosto 2013
Última Revisión: Marzo 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo de realización: 35 minutos.

Objetivo

Conocer el funcionamiento de la autoconfiguración sin estado (Stateless) y la forma de poder realizar su implementación en el software de simulación de redes GNS3.

Desarrollo

Nota: Los ruteadores seleccionaos para esta práctica son del modelo Cisco© 2691, cuya imagen del sistema operativo (IOS) no viene incluida previamente en el software GNS3, por lo que deberá solicitar la misma al instructor. Su uso es para fines académicos y únicamente podrá utilizarse para esta práctica.

Creación de la Topología de Red

Agregar las imágenes de las PC y los ruteadores al área de trabajo de GNS3, de tal manera que la topología quede de la siguiente forma: (ver figura 1).

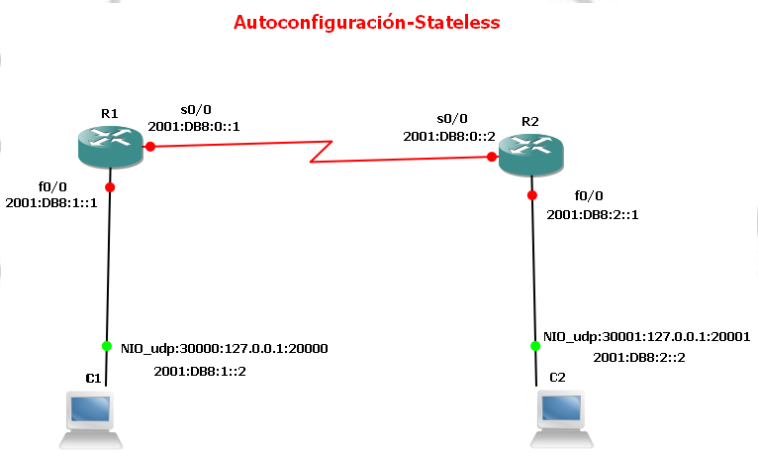


Figura 1. Ejemplo de la topología de red.

Configuración de los ruteadores

a) En la terminal del ruteador 1 teclear los siguientes comandos para configurar las interfaces del mismo con las direcciones IPv6 correspondientes, y activar la autoconfiguración stateless (ver tabla 1).

Tabla 1. Comandos de configuración en la terminal del ruteador 1.

```
R1> enable
R1# configure terminal
R1 (config)# interface FastEthernet 0/0
R1 (config-if)# ipv6 address (dirección IPv6)/64 eui-64
R1(config-if)#ipv6 enable
R1 (config-if)# no shutdown
R1 (config-if)#interface Serial 0/0
R1 (config-if)# ipv6 address (dirección IPv6)/64
R1 (config-if)# no shutdown
```

Nota: Cabe señalar que para que la autoconfiguración se lleve a cabo, es neceario incluir las siguientes líneas de comandos (ver tabla 2), ya que **ipv6 unicast-routing** habilita IPv6 de manera global e **ipv6 route ::/0 S0/0** permite que haya comunicación entre todos los equipos de la topología.

Tabla 2. Otros comandos que permiten la configuración de ruteo en la terminal del ruteador 1.

```
R1 (config)# ipv6 route ::/0 S0/0
R1 (config)#ipv6 unicast-routing
```

b) Repetir los comandos para el otro ruteador pero con las direcciones IPv6 que le correspondan, en este caso (dirección IPv6 interfaz Ethernet del ruteador 2)/64 eui-64, (dirección IPv6 interfaz Serial del ruteador2)/64 y poner los resultados en la siguiente tabla.

c) Teclear el comando **show ipv6 int brief** en la terminal de los ruteadores 1 y 2 para observar las direcciones de la interfaz FastEthernet asignadas a cada uno. Poner los resultados obtenidos en la siguiente tabla:

R1
R2

d) Ejecutar el programa **vpcs** que viene incluido en la carpeta donde se instaló GNS3. Una vez abierta la terminal del software, teclear el comando **show**, con el cual se podrá observar que las direcciones de las PC se configurarán de manera automática por los ruteadores a partir de los prefijos incluidos en las direcciones IPv6 configuradas en los mismos (ver figura 2).

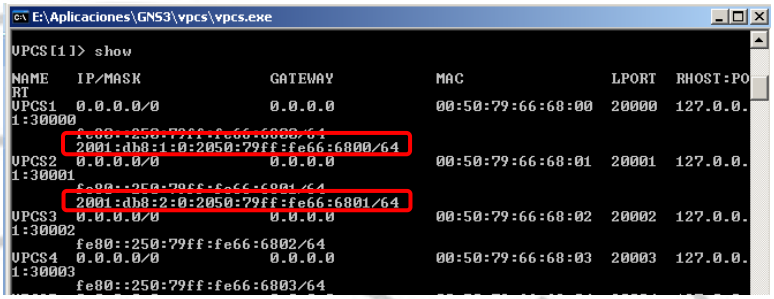


Figura 2. Ejecución del comando **show** en la terminal de vpcs.

e) Para verificar que hay conexión entre ambas PC teclear desde la terminal de la PC1 el comando **ping** a la dirección autoconfigurada de la PC 2 y realizar lo mismo desde la otra PC (escribiendo el número 2) hacia la PC 1 y poner los resultados obtenidos en la siguiente tabla:

PC1
PC2

f) También probar la conexión con el comando **ping** desde la terminal del ruteador 1 a la dirección que se autoconfiguró en la PC1 y poner los resultados obtenidos en la tabla siguiente:

R1

g) Realizar los mismos pasos de los incisos e) y f) pero en lugar de utilizar el comando **ping** usar el comando **trace** para ver cuál es el camino que siguen los paquetes enviados entre estos dispositivos, y poner los resultados obtenidos en la siguiente tabla:

PC1
PC2
R1

Explique cómo está conformada la dirección IPv6 que se le asignó a las PC:

_____

Práctica #6:

6.7 BGP en GNS3

Elaboración: Agosto 2013
Última Revisión: Marzo 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo estimado de realización: 40 minutos.

Objetivo

Conocer el funcionamiento del protocolo de ruteo BGP y la forma de poder realizar su implementación en el software de simulación de redes GNS3.

Desarrollo

Nota: Los ruteadores seleccionados para esta práctica son del modelo Cisco© 2691, cuya imagen del sistema operativo (IOS) no viene incluida previamente en el software GNS3, por lo que deberá solicitar la misma al instructor. Su uso es para fines académicos y únicamente podrá utilizarse para esta práctica.

Creación de la Topología de Red

Para esta práctica se usarán dos PC y dos ruteadores por lo que la topología deberá quedar como la siguiente figura 1.

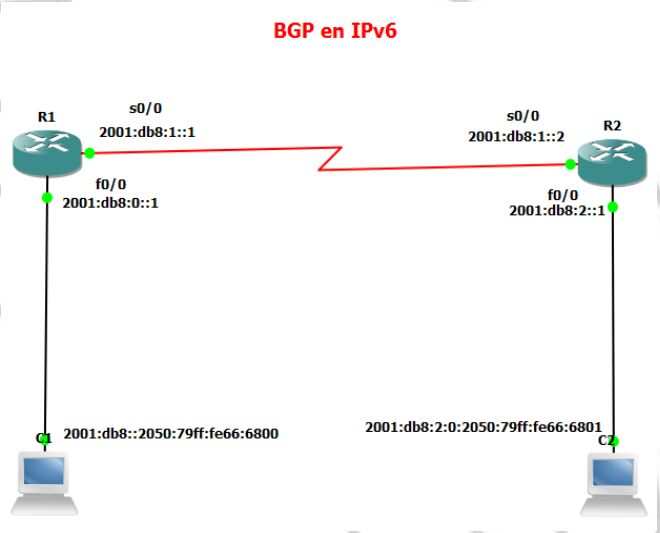


Figura 1. Ejemplo de la topología de red que se debe crear.

Configuración de los ruteadores

a) En la terminal del ruteador 1 teclear los siguientes comandos para configurar las interfaces del mismo con las direcciones IPv6 correspondientes, y activar la autoconfiguración stateless (ver tabla 1):

Tabla 1. Comandos de configuración en la terminal del ruteador 1.

```
R1> enable
R1# configure terminal
R1 (config)# ipv6 unicast-routing
R1 (config)# interface FastEthernet 0/0
R1 (config-if)# ipv6 address (dirección IPv6)/64 eui-64
R1(config-if)#ipv6 enable
R1 (config-if)# no shutdown
R1 (config-if)#interface Serial 0/0
R1 (config-if)# ipv6 address (dirección IPv6)/64
R1 (config-if)# no shutdown
```

b) Repetir los mismos pasos para el otro ruteador pero con las direcciones IPv6 que le correspondan, en este caso (dirección IPv6 interfaz Ethernet del ruteador 2)/64 eui-64, (dirección IPv6 interfaz Ethernet del ruteador 2)/64 (dirección IPv6 interfaz Serial del ruteador2)/64, y poner los resultados en la siguiente tabla:

Verificar que las direcciones IPv6 se configuraron correctamente en las interfaces de las PC con el comando **show** (ver figura 2).

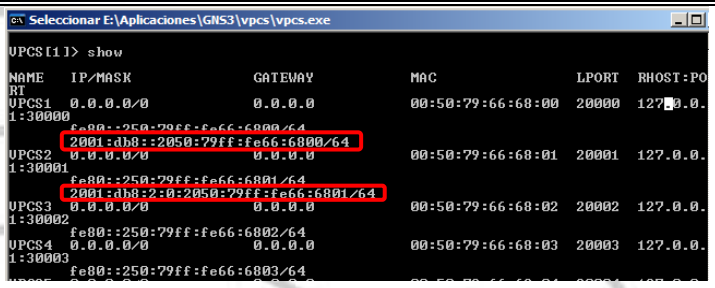


Figura 2. Ejecución del comando **show** en la terminal de VPCS.

c) En la terminal del ruteador 1 se habilitará BGP con los siguientes comandos (ver tabla 2):

Tabla 2. Comandos de configuración de BGP en la terminal del ruteador 1.

R1 >enable R1 #configure terminal R1(config)#router bgp **65001** R1(config-router)# no bgp default ipv4-unicast R1(config-router)#bgp router-id **1.1.1.1** R1(config-router)#neighbor ***(dirección IPv6 vecino)*** remote-as **65002** R1(config-router)#address-family ipv6 R1(config-router-af)#neighbor ***(dirección IPv6 vecino)*** activate R1(config-router-af)#network ***(dirección IPv6 de la red a anunciar)*** /48 R1(config-router)#redistribute connected R1(config-router-af)#exit-address-family

d) Realizar la misma configuración para el ruteador 2 pero con las diferentes direcciones IPv6, para llegar al ruteador 1 y poner los resultados obtenidos en la siguiente tabla:

R2

e) Teclear el comando **show bgp ipv6 unicast summary** en la terminal ambos ruteadores para observar, de forma resumida, las características configuradas de BGP en los mismos. Poner los resultados obtenidos en la siguiente tabla:

R1
R2

f) En la terminal de ambos ruteadores teclear el comando **show bgp ipv6 unicast neighbors** ***(dirección IPv6 vecino)*** **advertised-routes** para observar las redes que le anuncia cada ruteador a su vecino.

Poner los resultados obtenidos en la siguiente tabla:

R1
R2

g) Para observar las redes que le son anunciadas a cada ruteador por su vecino, teclear el comando **show bgp ipv6 unicast neighbors** ***(dirección IPv6 vecino)*** **routes** en la terminal de ambos ruteadores y poner los resultados obtenidos en la siguiente tabla:

R1
R2

h) Para verificar que hay conexión entre ambas PC teclear desde la terminal de la PC1 el comando **ping** a la dirección autoconfigurada de la PC 2 y poner los resultados obtenidos en la siguiente tabla:

i) También probar la conexión con el comando **ping** desde la terminal del ruteador 1 a la dirección FastEthernet del ruteador 2 y a la dirección que se autoconfiguró en la PC 2. Poner los resultados obtenidos en la siguiente tabla:

j) Realizar los mismos pasos del inciso anterior pero en lugar de utilizar el comando **ping** usar el comando **trace** para ver cuál es el camino que siguen los paquetes enviados entre estos dispositivos y poner los resultados obtenidos en la siguiente tabla:

PC1
R1

¿Qué línea de comando del paso 1 habilita IPv6 de manera global?

_____

Práctica #7:

6.8 Túnel con Autoconfiguración y ruteo estático en GNS3

Elaboración: Agosto 2013
Última Revisión: Marzo 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo estimado de realización: 50 minutos.

Objetivo

Conocer el funcionamiento de un túnel y aprender la forma de poder realizar su implementación en el software de simulación de redes GNS3.

Desarrollo

Nota: Los ruteadores seleccionados para esta práctica son del modelo Cisco© 2691 y 2600, cuyas imágenes del sistema operativo (IOS) no vienen incluidas previamente en el software GNS3, por lo que deberá solicitar las mismas al instructor. Su uso es para fines académicos y únicamente podrán utilizarse para esta práctica.

Creación de la Topología de Red

La topología que se debe crear deberá quedar de la siguiente forma (ver figura 1):

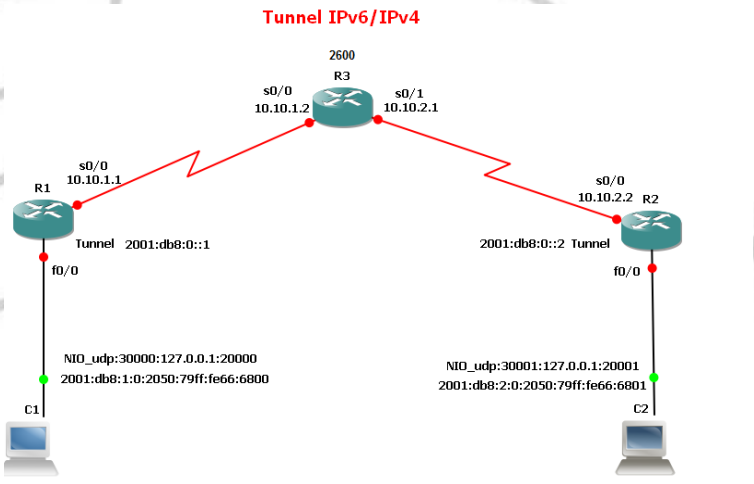


Figura 1. Ejemplo de topología de red final.

Configuración de los ruteadores.

a) En la terminal del ruteador 1 teclear los siguientes comandos para configurar las interfaces del mismo con las direcciones IPv6 e IPv4 (dual stack) correspondientes, y activar la autoconfiguración stateless (ver tabla 1):

Tabla 1. Comandos de configuración de las interfaces en la terminal del ruteador 1.

R1> enable R1# configure terminal R1 (config)#ipv6 unicast-routing R1 (config)# interface FastEthernet 0/0 R1 (config-if)# ipv6 address ***(dirección IPv6)***/64 eui-64 R1 (config-if)# ipv6 address ***(dirección IPv6)***/64 R1(config-if)#ipv6 enable R1 (config-if)# no shutdown R1 (config-if)#exit R1 (config)#interface Serial 0/0 R1 (config-if)# ip address ***(dirección IPv4) (mascara de red)*** R1 (config-if)# no shutdown

b) Configurar también una ruta estática por defecto, en la terminal del ruteador 1, en IPv4 con el siguiente comando (ver tabla 2):

Tabla 2. Comandos de configuración de una ruta estática en la terminal del ruteador 1.

R1 (config)#ip route 0.0.0.0 **0.0.0.0** S0/0

c) Repetir los mismos pasos de los incisos a) y b) para el ruteador 2 pero con las direcciones IPv6 e IPv4 que le correspondan, en este caso (dirección IPv6 interfaz Ethernet del ruteador 2)/64 eui-64, (dirección IPv6 interfaz Ethernet del ruteador 2)/64, (dirección IPv4 interfaz Serial del ruteador 2)/64 y poner los resultados obtenidos, en la terminal del ruteador, en la siguiente tabla:

a)
b)

d) En la terminal del ruteador 3 teclear los siguientes comandos para configurar las interfaces del mismo con las direcciones IPv4 correspondientes (ver tabla 3):

Tabla 3. Comandos de configuración de las interfaces en la terminal del ruteador 3.

R3> enable R3# configure terminal R3 (config-if)#interface Serial 0/0 R3 (config-if)# ip address ***(dirección IPv4) (máscara de red)*** R3 (config-if)# no shutdown R3 (config-if)# exit R3 (config)#interface Serial 0/1 R3 (config-if)# ip address ***(dirección IPv4) (máscara de red)*** R3 (config-if)# no shutdown

e) Configurar también dos rutas estáticas en IPv4 por defecto en la terminal del ruteador 3 para cada subred (como en el inciso b pero ahora serán dos rutas) y poner los resultados obtenidos en la siguiente tabla:

f) Ejecutar el programa **vpcs** que viene incluido en la carpeta donde se instaló GNS3. Una vez abierta la terminal del software teclear el comando **show**, con el cual se podrá observar que las direcciones de las PC se configurarán de manera automática por los ruteadores a partir de los prefijos incluidos en las direcciones IPv6 configuradas en los mismos (ver figura 2).

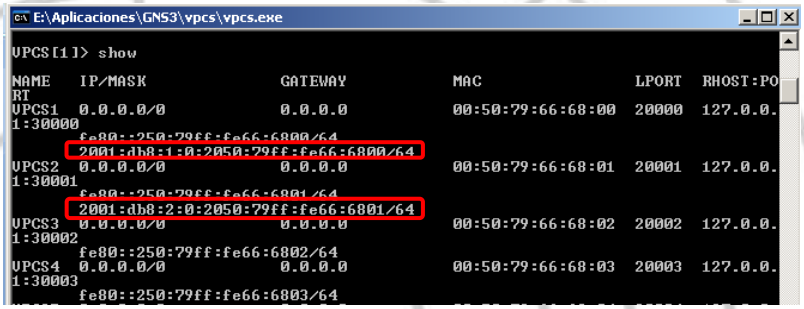


Figura 2. Ejecución del comando **show** en la terminal de **vpcs**.

Configuración de túneles.

g) Para realizar la configuración de un túnel en la terminal del ruteador 1 teclear los siguientes comandos:

Tabla 4. Comandos de configuración de un túnel en la terminal del ruteador 1.

R1# configure terminal R1(config)# interface tunnel 1 R1(config-if)#ipv6 address **(*dirección IPv6 origen*)**/64 R1(config-if)#description Tunel R1-R2 R1(config-if)#tunnel source s0/0 R1(config-if)#tunnel destination **(*dirección IPv4 destino R2*)** R1(config-if)#tunnel mode ipv6ip

h) Realizar la misma configuración para el ruteador 2 pero con diferentes direcciones IP, para llegar al ruteador 1 y poner los resultados obtenidos en la siguiente tabla:

R2

i) Teclear el comando **show ipv6 int brief** en la terminal de los ruteadores 1 y 2 para observar la interfaz **tunnel** que se configuró en los mismos. Poner los resultados obtenidos en la siguiente tabla:

R1
R2

j) Configurar también una ruta estática por defecto en IPv6 en la terminal del ruteador 1 con el siguiente comando (ver tabla 5):

Tabla 5. Comandos de una ruta estática en la interfaz de túnel en la terminal del ruteador 1.

R1 (config)# ipv6 route ::/0 Tunnel1

k) Al igual que en al inciso anterior, configurar una ruta estática por defecto en IPv6 en la terminal del ruteador 2 con el siguiente comando (ver tabla 6):

Tabla 6. Comandos de una ruta estática en la interfaz de túnel en la terminal del ruteador 2.

R2 (config)# ipv6 route ::/0 Tunnel1

l) Teclear el comando **show IPv6 route** en la terminal de ambos ruteadores y poner los resultados obtenidos en la siguiente tabla:

R1
R2

m) Para verificar que hay conexión entre ambas PC teclear desde la terminal de la PC1 el comando **ping** a la dirección autoconfigurada de la PC 2, realizar lo mismo desde la PC 2 (escribiendo el número 2) hacia la PC 1 y poner los resultados obtenidos en la siguiente tabla:

PC1
PC2

n) También probar la conexión con el comando **ping** desde la terminal del ruteador 1 a la dirección que se autoconfiguró en la PC1 y desde la PC1 hacia el ruteador. Poner los resultados obtenidos en la tabla siguiente:

R1
PC1

o) Realizar los mismos pasos de los dos incisos anteriores pero en lugar de utilizar el comando **ping** usar el comando **trace** para ver cuál es el camino que siguen los paquetes enviados entre estos dispositivos, y poner los resultados obtenidos en la siguiente tabla:

PC1
PC2
R1

Teclear el comando **show ipv6 tunnel** en las terminales de los ruteadores 1 y 2. Poner los resultados obtenidos en la siguiente tabla:

R1
R2

¿Cuáles son los tres métodos de transición que se usan actualmente para pasar de IPv4 a IPv6?

_____
_____
_____

Práctica #8:

6.9 Túnel con Autoconfiguración, RIPng y RIP en GNS3

Elaboración: Septiembre 2013
Última Revisión: Marzo 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo estimado de realización: 1 hora con 10 minutos.

Objetivo

Conocer el funcionamiento de un túnel IPv6 sobre IPv4 y aprender la forma de poder realizar su implementación con RIP y RIPng en el software de simulación de redes GNS3.

Desarrollo

Nota: Los ruteadores seleccionados para esta práctica son del modelo Cisco© 2691 y 2600, cuyas imágenes del sistema operativo (IOS) no vienen incluidas previamente en el software GNS3, por lo que deberá solicitar las mismas al instructor. Su uso es para fines académicos y únicamente podrán utilizarse para esta práctica.

Creación de la Topología de Red

Agregar las imágenes de las PC y los ruteadores al área de trabajo de GNS3. Se deberán agregar dos ruteadores del modelo 2691 y uno del modelo 2600 (ver figura 1).

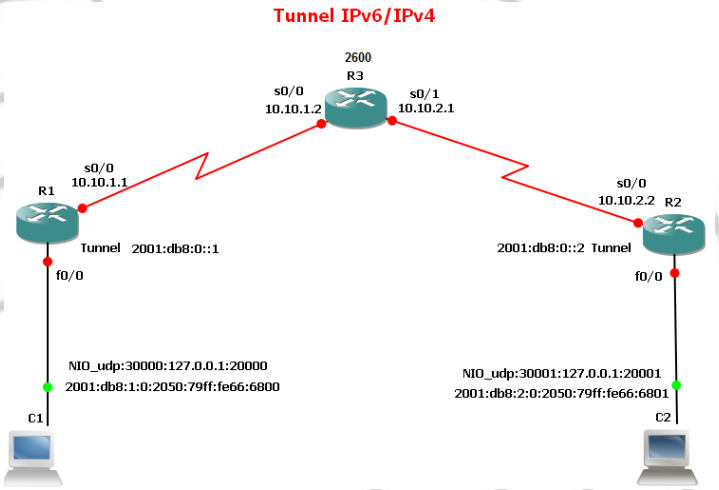


Figura 1. Ejemplo de topología de red a crear.

Configuración de los ruteadores

a) En la terminal del ruteador 1 teclear los siguientes comandos para configurar las interfaces del mismo con las direcciones IPv6 e IPv4 (dual stack) correspondientes, y activar la autoconfiguración stateless (ver tabla 1):

Tabla 1. Comandos de configuración de las interfaces en la terminal del ruteador 1.

R1> enable R1# configure terminal R1 (config)#ipv6 unicast-routing R1 (config)# interface FastEthernet 0/0 R1 (config-if)# ipv6 address ***(dirección IPv6)***/64 eui-64 R1 (config-if)# ipv6 address ***(dirección IPv6)***/64 R1(config-if)#ipv6 enable R1 (config-if)# no shutdown R1 (config-if)#exit R1 (config)#interface Serial 0/0 R1 (config-if)# ip address ***(dirección IPv4) (mascara de red)*** R1 (config-if)# no shutdown

b) Configurar también RIP en la terminal del ruteador 1 con los siguientes comandos (ver tabla 2):

Tabla 2. Comandos de configuración de **RIP** en la terminal del ruteador 1

R1#configure terminal R1(config)#router **rip** R1(config-router)#network ***(dirección IPv4 del ruteador vecino)***

c) Repetir los mismos pasos de los incisos a) y b) para el ruteador 2 pero con las direcciones IPv6 e IPv4 que le correspondan, y poner los resultados obtenidos en la siguiente tabla.

a)
b)

d) En la terminal del ruteador 3 teclear los siguientes comandos para configurar las interfaces del mismo con las direcciones IPv4 correspondientes (ver tabla 3):

Tabla 3. Comandos de configuración de las interfaces en la terminal del ruteador 3.

```
R3> enable
R3# configure terminal
R3 (config-if)#interface Serial 0/0
R3 (config-if)# ip address (dirección IPv4) (máscara de red)
R3 (config-if)# no shutdown
R3 (config-if)# exit
R3 (config)#interface Serial 0/1
R3 (config-if)# ip address (dirección IPv4) (máscara de red)
R3 (config-if)# no shutdown
```

e) Configurar también RIP en la terminal del ruteador 3 (como en el inciso "b") y poner los resultados obtenidos en la siguiente tabla:

Nota: Para el ruteador 3 se deberán introducir dos direcciones IPv4 de ruteadores vecinos ya que tiene 2 ruteadores colindantes con él.

En la terminal de configuración de las PC teclear el comando show, con el cual se podrá observar que las direcciones de las PC se configuraron de manera automática por los ruteadores a partir de los prefijos incluidos en las direcciones IPv6 configuradas en los mismos (ver figura 2).

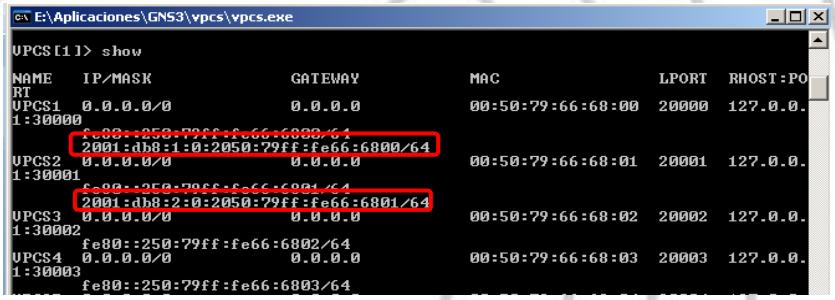


Figura 2. Ejecución del comando **show** en la terminal de **vpcs**.

Configuración de túneles.

f) Para realizar la configuración de un túnel en la terminal del ruteador 1 teclear los siguientes comandos:

Tabla 4. Comandos de configuración de un túnel en la terminal del ruteador 1.

R1# configure terminal
R1(config)# interface tunnel 1
R1(config-if)#ipv6 address (dirección IPv6 origen)/64
R1(config-if)#description Tunel R1-R2
R1(config-if)#tunnel source s0/0
R1(config-if)#tunnel destination (dirección IPv4 destino R2)
R1(config-if)#tunnel mode ipv6ip

g) Realizar la misma configuración para el ruteador 2 pero con diferentes direcciones IP, para llegar al ruteador 1 y poner los resultados obtenidos en la siguiente tabla:

R2

h) Teclear el comando **show ipv6 int brief** en la terminal de los ruteadores 1 y 2 para observar la interfaz **tunnel** que se configuró en los mismos. Poner los resultados obtenidos en la siguiente tabla:

R1
R2

i) Habilitar la configuración de RIPng en la terminal del ruteador 1, para que haya comunicación IPv6 entre algunos de los dispositivos de la topología con los siguientes comandos (Ver tabla 5):

Tabla 5. Configuración de **RIPng** en la terminal del ruteador 1.

R1 >enable R1 #configure terminal R1 (config)# ipv6 unicast-routing R1 (config)# ipv6 router rip **proceso tunel** R1 (config)# interface tunnel1 R1 (config-if)# ipv6 rip **proceso tunel** enable R1(config-if)#ipv6 rip **proceso tunel default-information originate** R1 (config-if)# exit R1(config)# ipv6 router rip **proceso tunel** R2(config-rtr)#**redistribute connected**

j) Al igual que en el inciso anterior, configurar RIPng pero en la terminal del ruteador 2 y poner los resultados obtenidos en la siguiente tabla:

k) Teclear el comando **show IPv6 route** en la terminal de ambos ruteadores y poner los resultados obtenidos en la siguiente tabla:

R1
R2

l) Para verificar que hay conexión entre ambas PC teclear desde la terminal de la PC 1 el comando **ping** a la dirección autoconfigurada de la PC 2, y realizar lo mismo desde la PC 2 (escribiendo el número 2) hacia la PC 1 y poner los resultados obtenidos en la siguiente tabla:

PC1
PC2

m) También probar la conexión con el comando **ping** desde la terminal del ruteador 1 a la dirección que se autoconfiguró en la PC 1 y desde la PC 1 hacia el ruteador. Poner los resultados obtenidos en la tabla siguiente:

R1
PC1

n) Teclear el comando **show ipv6 tunnel** en las terminales de los ruteadores 1 y 2**, y** poner los resultados obtenidos en la siguiente tabla:

R1
R2

o) Teclear el comando **show ip route** en la terminal de los 3 ruteadores y poner los resultados obtenidos en la siguiente tabla:

R1
R2
R3

p) Como parte adicional de la práctica, agregar a la topología de red dos PC con IPv4 conectadas a los dos ruteadores que manejan pila dual. La topología quedará de la siguiente forma (ver figura 3):

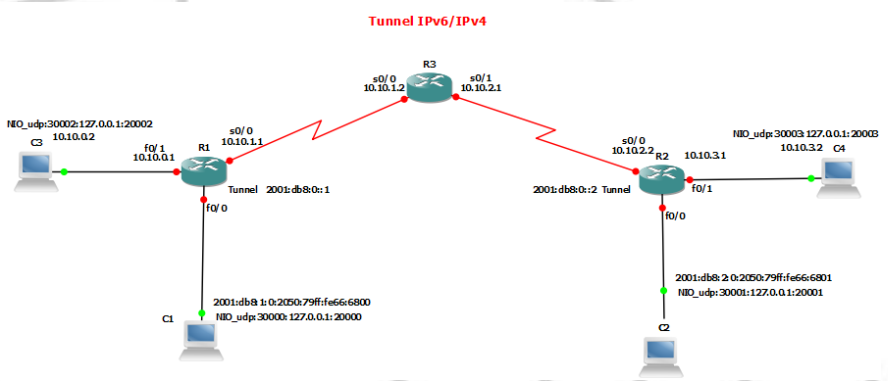


Figura 3. Ejemplo de topología final con 4 PC y 3 ruteadores.

q) Probar la conectividad por IPv4 desde la PC 3 a la PC 4 con el comando **ping** y desde la PC 4 hacia la PC 3. Poner los resultados obtenidos en la siguiente tabla:

PC3
PC4

r) Repetir el inciso anterior pero en lugar de usar el comando **ping** usar **trace** para ver cuál es el camino que siguen los paquetes enviados entre estos dispositivos y poner los resultados obtenidos en la siguiente tabla:

PC3
PC4

Práctica #9:

6.10 Túnel con Autoconfiguración y BGP en GNS3

Elaboración: Septiembre 2013
Última Revisión: Marzo 2014
Última Actualización: Marzo 2014

Elaboraron: Ing. Manuel Alejandro Ponce Monterrosas
Ing. Azael Fernández Alcántara

Tiempo estimado de realización: 50 minutos.

Objetivo

Conocer el funcionamiento de un túnel IPv6 sobre IPv4 y aprender la forma de poder realizar su implementación con BGP en el software de simulación de redes GNS3.

Desarrollo

Nota: Los ruteadores seleccionados para esta práctica son del modelo Cisco© 2691 y 2600, cuyas imágenes del sistema operativo (IOS) no vienen incluidas previamente en el software GNS3, por lo que deberá solicitar las mismas al instructor. Su uso es para fines académicos y únicamente podrán utilizarse para esta práctica.

Creación de una Topología de Red

Se deberán agregar dos ruteadores del modelo 2691 y uno del modelo 2600, se usarán dos PC por lo que se añadirán dos símbolos de las mismas al área de trabajo.
La topología finalmente quedará de la siguiente forma (ver figura 1).

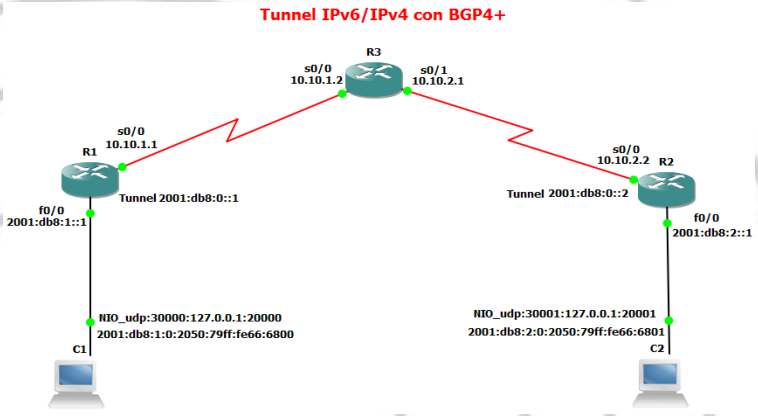


Figura 1. Ejemplo de topología de red final.

Configuración de los ruteadores

a) En la terminal del ruteador 1 teclear los siguientes comandos para configurar las interfaces del mismo con las direcciones IPv6 e IPv4 (dual stack) correspondientes, y activar la autoconfiguración stateless (ver tabla 1):

Tabla 1. Comandos de configuración de las interfaces en la terminal del ruteador 1.

```
R1> enable
R1# configure terminal
R1 (config)# interface FastEthernet 0/0
R1 (config-if)# ipv6 address (dirección IPv6)/64 eui-64
R1 (config-if)# ipv6 address (dirección IPv6)/64
R1(config-if)#ipv6 enable
R1 (config-if)# no shutdown
R1 (config-if)#exit
R1 (config)#interface Serial 0/0
R1 (config-if)# ip address (dirección IPv4) (máscara de red)
R1 (config-if)# no shutdown
```

Nota: Cabe señalar que para que la autoconfiguración se lleve a cabo, es necesario incluir la línea de comando **ipv6 unicast-routing** ya que habilita IPv6 de manera global.

b) Repetir el inciso anterior para el ruteador 2 pero con las direcciones IPv6 e IPv4 que le correspondan y poner los resultados que obtenidos en la terminal de este en la siguiente tabla.

c) En la terminal del ruteador 3 teclear los siguientes comandos para configurar las interfaces del mismo con las direcciones IPv4 correspondientes (ver tabla 2):

Tabla 2. Comandos de configuración de las interfaces en la terminal del ruteador 3.

```
R3> enable
R3# configure terminal
R3 (config-if)#interface Serial 0/0
R3 (config-if)# ip address (dirección IPv4) (máscara de red)
R3 (config-if)# no shutdown
R3 (config-if)# exit
R3 (config)#interface Serial 0/1
R3 (config-if)# ip address (dirección IPv4) (máscara de red)
R3 (config-if)# no shutdown
```

d) Comprobar con el comando **show**, en la terminal de las PC, que sus interfaces se configuraron de manera automática por los ruteadores a partir de los prefijos incluidos en las direcciones IPv6 configuradas en los mismos (ver figura 2).

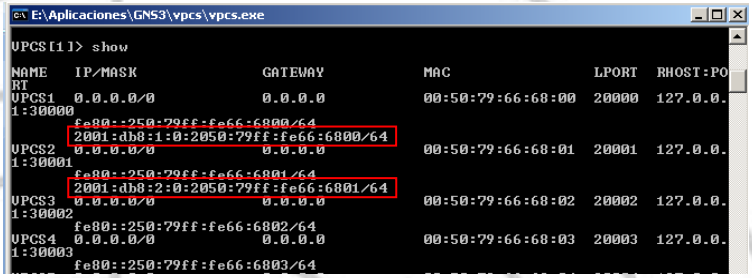


Figura 2. Ejecución del comando **show** en la terminal de **vpcs**.

Configuración de túneles.

e) Para realizar la configuración de un túnel IPv6 sobre IPv4 en la terminal del ruteador 1 teclear los siguientes comandos:

Tabla 3. Comandos de configuración de un túnel en la terminal del ruteador 1.

R1# configure terminal R1(config)# interface **tunnel 1** R1(config-if)#ipv6 address **(*dirección IPv6 origen*)**/64 R1(config-if)#description **Tunel R1-R2** R1(config-if)#tunnel source s0/0 R1(config-if)#tunnel destination **(*dirección IPv4 destino R2*)** R1(config-if)#tunnel mode ipv6ip

f) Realizar la misma configuración para el ruteador 2 pero con diferentes direcciones IP, para llegar al ruteador 1 y poner los resultados obtenidos en la siguiente tabla:

R2

g) Teclear el comando **show ipv6 int brief** en la terminal de los ruteadores 1 y 2 para observar la interfaz **tunnel** que se configuró en los mismos. Poner los resultados obtenidos en la siguiente tabla:

R1
R2

h) Habilitar BGP con IPv4 en la terminal del ruteador 1 para que haya comunicación (en IPv4) entre los ruteadores de la topología con los siguientes comandos (ver tabla 4):

Tabla 4. Configuración de BGP con IPv4 en la terminal del ruteador 1.

R1 >enable R1 #configure terminal R1(config)#router bgp **65001** R1(config-router)#bgp router-id **1.1.1.1** R1(config-router)#neighbor ***(dirección IPv4 vecino)*** remote-as **65002** R1(config-router)#address-family ipv4 R1(config-router-af)#neighbor ***(dirección IPv4 vecino)*** activate R1(config-router-af)#network ***(dirección IPv4 de la red a anunciar)*** R1(config-router)#redistribute connected R1(config-router-af)#exit-address-family

i) Al igual que en el inciso anterior, configurar BGP con IPv4 pero ahora hacerlo en la terminal de los ruteadores 2 y 3. Poner los resultados obtenidos en la siguiente tabla:

R2
R3

j) Habilitar BGP con IPv6 en la terminal del ruteador 1 para que haya comunicación entre los ruteadores 1 y 2 y las PC que se comunican por medio de IPv6, con los siguientes comandos (ver tabla 5):

Tabla 5. Configuración de BGP con IPv6 en la terminal del ruteador 1

```
R1 >enable
R1 #configure terminal
R1(config)#router bgp 65001
R1(config-router)#bgp router-id 1.1.1.1
R1(config-router)#neighbor (dirección IPv6 vecino) remote-as 65002
R1(config-router)#address-family ipv6
R1(config-router-af)#neighbor (dirección IPv6 vecino)  activate
R1(config-router-af)#network (dirección IPv6 de la red a anunciar) /48
R1(config-router)#redistribute connected
R1(config-router-af)#exit-address-family
```

k) Repetir el inciso anterior para configurar BGP con IPv6 pero en la terminal del ruteador 2. Poner los resultados obtenidos en la siguiente tabla:

R2

l) Teclear el comando **show bgp ipv6 unicast summary** en la terminal de los ruteadores 1 y 2 para observar, de forma resumida, las características configuradas de BGP con IPv6 en los mismos. Poner los resultados obtenidos en la siguiente tabla:

R1
R2

m) Después teclear el comando **show ip bgp summary** en la terminal de los 3 ruteadores para observar, de forma resumida, las características configuradas de BGP con IPv4. Poner los resultados obtenidos en la siguiente tabla:

R1
R2
R3

n) Para verificar que hay conexión entre ambas PC teclear desde la terminal de la PC 1 el comando **ping** a la dirección autoconfigurada de la PC 2 y realizar lo mismo desde la PC 2 hacia la PC 1 y poner los resultados obtenidos en la siguiente tabla:

PC1
PC2

o) También probar la conexión con el comando **ping** desde la terminal del ruteador 1 a la dirección que se autoconfiguró en la PC 1 y desde la PC 1 hacia el ruteador 1. Poner los resultados obtenidos en la tabla siguiente:

R1
PC1

p) Realizar los mismos pasos de los incisos n) y o) pero en lugar de utilizar el comando **ping** usar el comando **trace** para ver cuál es el camino que siguen los paquetes enviados entre estos dispositivos y poner los resultados obtenidos en la siguiente tabla:

PC1
PC2
R1

Capítulo 7. Uso de las prácticas en casos reales y resultados obtenidos

7.1 Introducción

Como parte del análisis iniciado durante mi estancia en el servicio social y continuado al realizar este trabajo, se usaron algunas de las prácticas descritas en el capítulo anterior en ambientes académicos reales (no se usaron todas las demás prácticas debido a falta de tiempo disponible para aplicarlas dentro del curso), en dos grupos de clase: alumnos del "Diplomado Integral de Telecomunicaciones" impartido por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) en las instalaciones de la misma, y en un grupo de becarios de la Dirección de Telecomunicaciones de la propia dependencia. Con el fin ayudarlos en su formación de las redes de datos, en particular en el tema de IPv6, para aplicar los conocimientos adquiridos en la teoría, mediante el software GNS3. Es por ello que se tomaron las primeras cinco prácticas de ese capítulo para ser aplicadas en un ambiente real probando su eficiencia y funcionalidad.

Las prácticas que se solicitó a los alumnos realizar, con el fin de tomar nota de las dificultades para realizarlas y el tiempo requerido, fueron las siguientes:

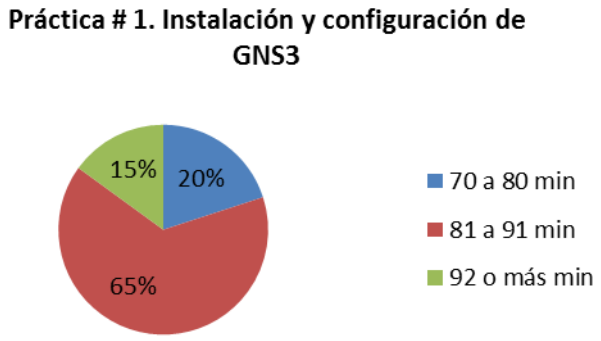
- Instalación y configuración de GNS3
- Ruteo estático con IPv4 e IPv6 en GNS3
- RIP en GNS3
- RIPng en GNS3
- Autoconfiguración Stateless en GNS3

7.2 Resultados de las pruebas

Se obtuvieron resultados importantes en el desempeño de los alumnos, los cuales se muestran a continuación por medio de unas gráficas para indicar de forma visual los mismos

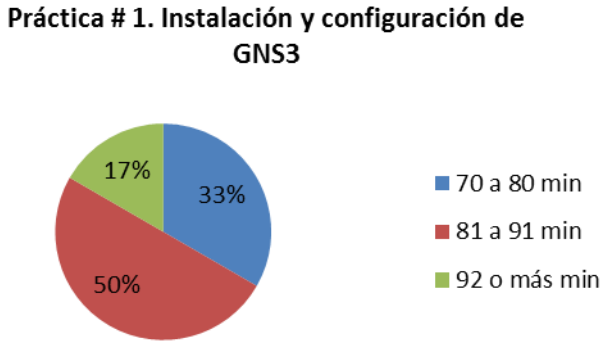
Se presenta una gráfica por grupo y una que contiene la suma de alumnos de ambos grupos (solo para las primeras dos prácticas).

Tiempo en realizar las prácticas.



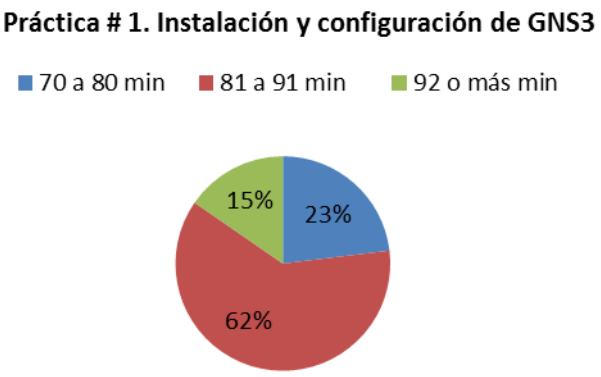
Gráfica 1. Porcentaje de alumnos del diplomado, de acuerdo a los tiempos de realización de la práctica #1.

La gráfica anterior muestra que el 20 por ciento de los alumnos del grupo del diplomado, terminó la práctica número uno entre los primeros 70 a 80 minutos y que más de la mitad, es decir el 65 por ciento, la realizó entre los 81 a 91 minutos, quedando el 15 por ciento, el cual la concluyó después de los 91 minutos.



Gráfica 2. Porcentaje de alumnos del grupo de becarios, de acuerdo a los tiempos de realización de la práctica #1.

En la gráfica 2 aparece que el resultado de la aplicación de la práctica número uno al grupo de becarios, arrojó como resultado que el 33 por ciento de los alumnos acabó la práctica en un tiempo de 70 a 80 minutos, el 50 por ciento entre los 81 a 91 minutos y el 17 por ciento restante la terminó en más de 91 minutos.

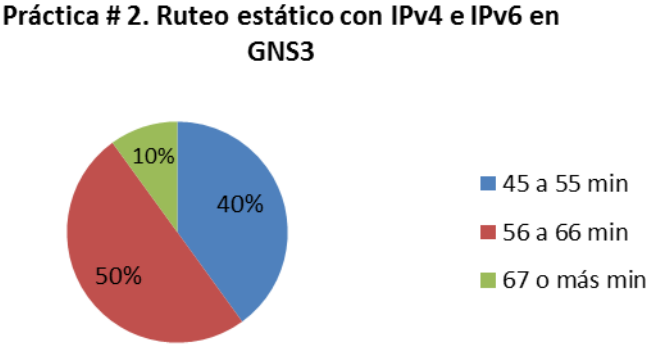


Gráfica 3. Porcentaje de alumnos de ambos grupos, de acuerdo a los tiempos de realización de la práctica #1.

Los resultados que muestra la gráfica 3 son el porcentaje de la suma de los alumnos de ambos grupos, que terminaron la práctica en un tiempo determinado, específicamente se muestra que el 23 por ciento la realizó en el rango de tiempo de los 70 a 80 minutos, el 62 por ciento entre 81 y 91 minutos y en más de 91 minutos el 15 por ciento restante.

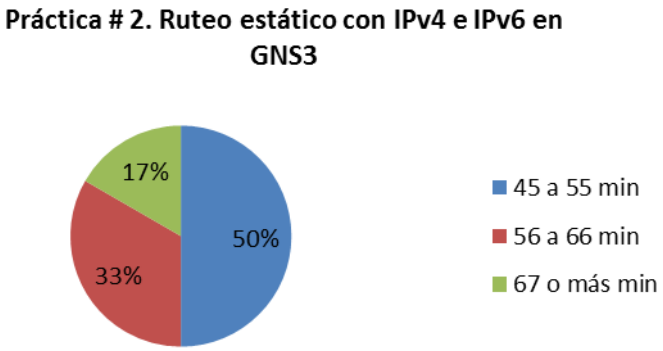
La práctica número 1, a pesar de ser muy sencilla pero resultar fundamental para la buena realización de las siguientes, les tomó un poco de tiempo a los alumnos concluirla ya que tenían que descargar el software, realizar los pasos de instalación y configuración del mismo. Otro aspecto que influyó en el tiempo de realización, fue que ninguno estaba familiarizado con este software en comparación con otros simuladores que no hay que configurarlos, solo instalarlos y usarlos.

En general ninguno de los alumnos tuvo algún problema considerable para realizar esta práctica.



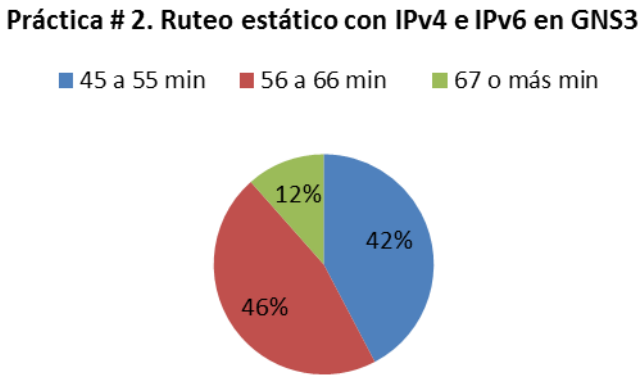
Gráfica 4. Porcentaje de alumnos del diplomado, de acuerdo a los tiempos de realización de la práctica #2.

Se puede visualizar en la gráfica 4 que el 40 por ciento de los alumnos del diplomado, terminó la práctica número dos entre los 45 y 55 minutos, el 50 por ciento en los 56 a 66 minutos y el 10 por ciento en más de 66 minutos.



Gráfica 5. Porcentaje de alumnos del grupo de becarios, de acuerdo a los tiempos de realización de la práctica #2.

Lo que dice la gráfica 5 es que el 50 por ciento hizo la práctica en un tiempo de 45 a 55 minutos, el 33 por ciento se llevó de 56 a 66 minutos y el 17 por ciento más de 66 minutos.



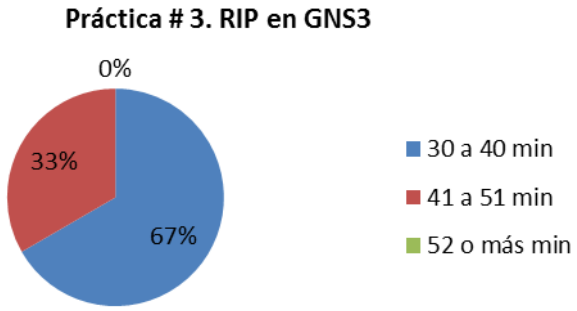
Gráfica 6. Porcentaje de alumnos de ambos grupos, de acuerdo a los tiempos de realización de la práctica #2.

Para el porcentaje de alumnos de ambos grupos, los tiempos que mostró la gráfica 6 son que el 42 por ciento necesitó de 45 a 55 minutos para realizarla, el 46 por ciento de 56 a 66 minutos y el 12 por ciento requirió de más de 66 minutos.

En esta práctica se les dificultó un poco más a algunos alumnos, el encontrar una asignación correcta de memoria para los equipos en la simulación con el parámetro **Idle PC,**

ya que no siempre se escogía la adecuada y esto hacía que el programa se congelara, debido a que estaban usando un ruteador que demandaba más recursos que el de la práctica anterior al requerirse ahora el soporte de IPv6.

No se les dificultó la parte de configuración de los ruteadores ya que es muy similar a como se realiza en simuladores como el Packet Tracer, software que la mayoría de los alumnos conocía. En general, se llevaron más tiempo en realizar esta práctica que la anterior debido a que aquí realizaron la configuración del ruteo tanto en IPv4 como en IPv6.

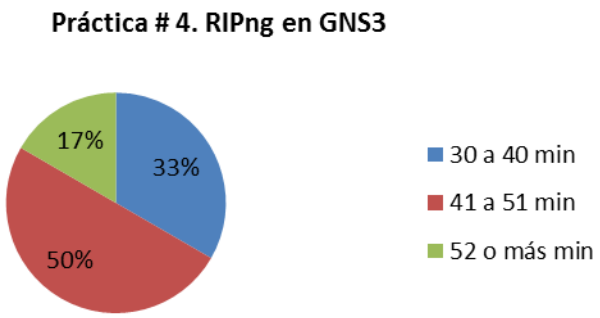


Gráfica 7. Porcentaje de alumnos del grupo de becarios, de acuerdo a los tiempos de realización de la práctica #3.

De los alumnos del grupo de becarios, se obtuvo la gráfica 7 de resultados al realizar la práctica número 3, donde se puede ver que el 67 por ciento de ellos terminó de realizarla en un tiempo de 30 a 40 minutos y el restante 33 por ciento la concluyó en el rango de 41 a 51 minutos. Todos terminaron antes de 52 minutos.

Cabe resaltar que a partir de esta práctica, solo la realizaron los alumnos del segundo grupo, es decir los del grupo de becarios, debido a falta de tiempo disponible, que ya no pudo otorgar el instructor del diplomado.

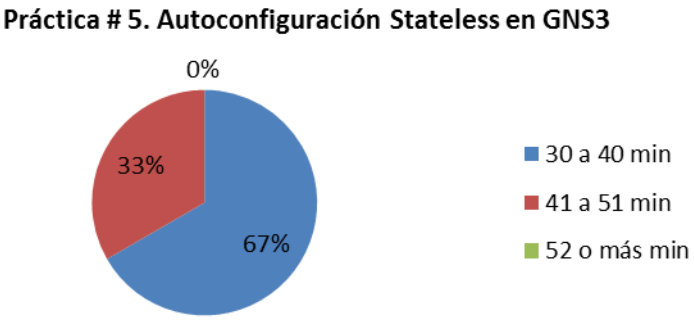
Esta práctica fue una de las más sencillas de realizar, no tuvieron problemas por los antecedentes del grupo, solo un poco de dificultad en responder las preguntas que vienen al final de la práctica.



Gráfica 8. Porcentaje de alumnos del grupo de becarios, de acuerdo a los tiempos de realización de la práctica #4.

Para la práctica 4 se obtuvieron los resultados que aparecen en la gráfica 8, donde el 33 por ciento concluyó la misma en un tiempo de entre 30 a 40 minutos, el 50 por ciento entre 41 y 51 minutos, el restante 17 por ciento requirió de más de 51 minutos.

Con la realización de esta práctica los alumnos entendieron mejor cuales son las diferencias entre IPv4 e IPv6, ya que en la práctica anterior configuraron RIP y en esta RIPng, que es la versión para IPv6, pudiendo así hacer comparaciones de forma práctica sobre ambas versiones de los protocolos a la hora de configurarlos en un ruteador.
Les llevó un poco más de tiempo que la anterior el poder realizarla, debido a que en esta se incluyó la captura de paquetes en una interfaz de una subred con el software **Wireshark**.



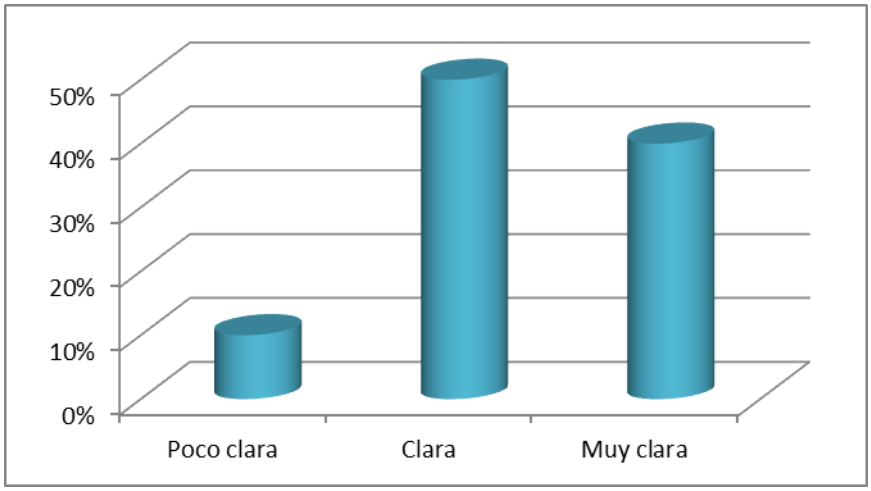
Gráfica 9. Porcentaje de alumnos del grupo de becarios, de acuerdo a los tiempos de realización de la práctica #5.

Lo que muestra la gráfica 9 es que el 67 por ciento realizó la práctica 5 en un tiempo de entre 30 a 40 minutos y el 33 por ciento restante se llevó un tiempo de 41 a 51 minutos. Nadie termino después de los 51 minutos.

En esta práctica, la mayoría de los alumnos tuvieron más problemas al realizar la autoconfiguración Stateless, ya que algunos olvidaban poner **eui-64** al final de la línea del comando y otros se confundían en que interfaz de red se tenía que seleccionar la autoconfiguración. Por lo demás, esta práctica se les hizo sumamente sencilla.

Apreciación de la claridad en las instrucciones de las prácticas por los estudiantes.

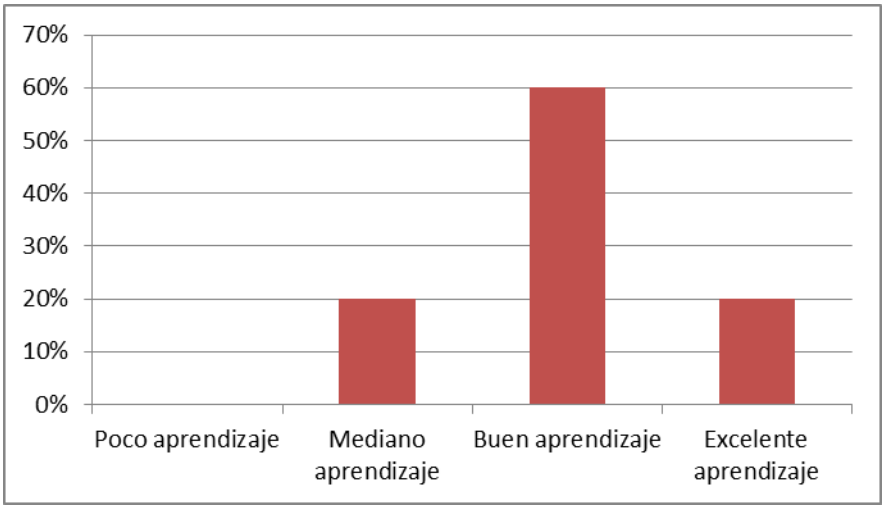
Durante y después de realizadas las prácticas se tomó nota del entendimiento de las instrucciones por parte de los alumnos para saber si estuvieron bien redactadas y se entendió lo que se tenía que realizar en cada una, considerando como factor de medición el número de preguntas con dudas.



Gráfica 10. Resultados de la apreciación de la claridad en las instrucciones de las prácticas por los estudiantes.

Percepción del impacto que tuvieron las prácticas en el aprendizaje de los estudiantes.

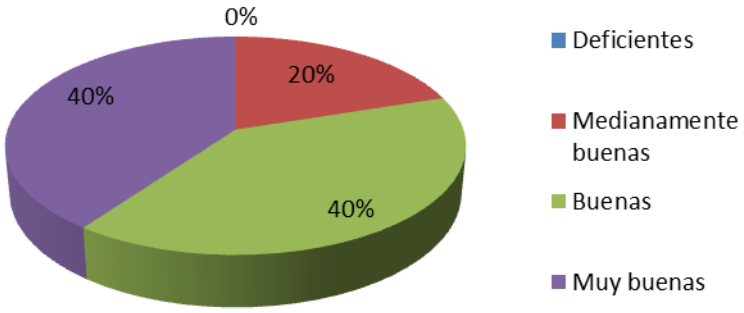
Se les preguntó a los alumnos de ambos grupos al término de haber realizado las prácticas, si consideraban que estas contribuyeron en algo a su aprendizaje, de lo que respondieron se obtuvo la gráfica 11.



Gráfica 11. Impacto que tuvieron las prácticas en el aprendizaje de los estudiantes.

Retroalimentación final de los alumnos sobre las prácticas

También se les preguntó a los alumnos sobre que les habían parecido las prácticas en general para así obtener una retroalimentación de las mismas, concluyendo en los resultados mostrados en la gráfica siguiente:



Gráfica 12. Resultados de como calificaron los alumnos a las prácticas de manera general.

La gráfica 12 muestra que el 40% de los alumnos consideró, en forma general, que las prácticas fueron muy buenas, el otro 40% las calificó como buenas y al 20% restante les parecieron medianamente buenas. Ninguno de los alumnos a los que se les pregunto dijeron que las prácticas les parecieron deficientes.

Capítulo 8. Conclusiones

Con la realización de este trabajo, las prácticas propuestas y la teoría presentada, obtenidas después de una ardua investigación y realización de pruebas, se espera ofrecer una opción de estudio que pueda apoyar a profesores, alumnos y a todas las personas que se relacionen con el tema de las redes de datos, a reforzar los conceptos de forma teórica y práctica, por medio de la herramienta de simulación GNS3, la cual se observó, ofrece varias ventajas sobre otros simuladores, como los mencionados en el desarrollo del presente.

Dado que al momento de investigar sobre este simulador se encontró poca información oficial, la mayoría en el idioma inglés, sobre cómo poder configurar al mismo y usar las demás características con las que cuenta, se piensa que este trabajo, colaborará con información clara y detallada sobre el uso de esta herramienta, permitiendo a los interesados no perder mucho tiempo en investigar al respecto, y más bien emplear ese periodo valioso para desarrollar otras actividades que contribuyan a su aprendizaje.

Como estudiante que fui, creo que una buena manera de exponer un tema es de forma práctica, es por ello que se diseñaron una serie de prácticas para hacer que el acercamiento a algunos temas teóricos de las materias de redes de datos, con la ayuda de este simulador, sea lo más simple posible, donde no solo se enseñe el uso de GNS3 sino también a poder configurar equipos como ruteadores, Switches y PC que soporten las 2 versiones del IP (IPv4 e IPv6 respectivamente); dado que además, considero que IPv6 careció de una correcta difusión y conocimiento, tanto práctico como teórico, a lo largo de mi carrera, a pesar de ser importante ya su enseñanza por estar soportado en prácticamente todos los sistemas operativos recientes, y tratarse de una tecnología que estará cada vez más presente en las redes de datos, por lo cual, los ingenieros de hoy en día deberán entender los principios y la forma de funcionar que conlleva esta versión de IP.

La aplicación en dos casos reales del uso de las prácticas mostró que contaron con una buena claridad al presentar las instrucciones, un adecuado entendimiento sobre los procedimientos que había que realizar y una correcta aceptación al considerarlas fáciles de realizar; tuvieron un impacto positivo que contribuyó con el aprendizaje de los alumnos, y disfrutaron un tiempo de resolución razonable. Por lo que se propone que se implementen en un futuro, en algún grupo de estudio de la Facultad de Ingeniería para colaborar con esta extensa área que son las redes de datos, en particular con el soporte de IPv6 en mente.

Glosario

IP	Protocolo de internet.
Autoconfiguración	Característica de IPv6 la cual permite asignar de forma automática, una o varias direcciones IPv6 a la interfaz de un equipo que se conecte a una red, que funcione con esta versión del protocolo.
Túneles	Mecanismo de transición de IPv4 a IPv6, el cual permite encapsular paquetes IPv6 con encabezados de IPv4 para transportarse por redes de IPv4.
Ethernet	Es un norma de redes de área local.
DSL	Línea Digital de Suscritor. Es una conexión con una compañía telefónica que permite también conectarse a Internet.
Dial-up	Tecnología que permite acceder al servicio de Internet a través de una línea telefónica analógica y un módem.
Datagrama	Es la agrupación lógica de información que se envía como una unidad de capa de red a través de un medio de transmisión**.**
QoS	Calidad de servicio.
Multi-hilo	Paradigma de programación que permite ejecutar tareas de manera concurrente o simultánea.
DARPA	Agencia de Proyectos de Investigación Avanzados de Defensa de los Estados Unidos.
Lenguajes de script	Son lenguajes que no necesitan ser compilados si no solo interpretados.
Perl	Lenguaje de programación que toma características del lenguaje C.

Tcl	Lenguaje de script que se utiliza principalmente para el desarrollo rápido de prototipos, aplicaciones "script", interfaces gráficas y pruebas.
Python	Lenguaje de programación interpretado.
OTcl	Es lo mismo que el lenguaje Tcl pero orientado a objetos.
TIC	Tecnologías de la información y comunicación.
Traducción	Mecanismo de transición que consiste en la traducción de paquetes IPv4-IPv6 en ambos sentidos.

Referencias

[1] Tanenbaum, A. (2003). *Redes de computadoras.* (4ª Ed). México: Prentice-Hall.

[2] Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L. y Lynch, D.C. (2012). *Breve historia de Internet.* Internet Society (ISOC).

[3] Young, C.E. (2012). *A standard session protocol for open systems interconnection (OSI).* IEEE.

[4] Tanenbaum, A. (2003). *Redes de computadoras.* (4ª Ed). México: Prentice-Hall.

[5] Herrera, E. (2010). *Tecnologías y redes de transmisión de datos.* México: Limusa.

[6] Russell, A. L. (2013). *How TCP/IP eclipsed the Open Systems Interconnection standards to become the global protocol for computer networking.* IEEE.

[7] Dye, M.A., McDonald, R. y Rufi, A. W. (2008). *Network Fundamentals*. USA: Cisco Press.

[8] Huidobro, J. M., Millán R. J. (2007). *Redes de Datos y Convergencia IP*. Creaciones copyright.

[9] IETF. (1981). *INTERNET PROTOCOL: DARPA INTERNET PROGRAM: PROTOCOL SPECIFICATION.* RFC 791

[10] IETF. (2013). *Updated Specification of the IPv4 ID Field*. RFC 6864.

[11] Red de grupo de trabajo. (1998). *Internet Protocol, Version 6 (IPv6): Specification.* RFC 2460.

[12] Fernández, A. (2010). *Tutorial de IPv6*. Proyecto y Grupo de trabajo de IPv6 de la UNAM, Capítulo Mexicano del Foro IPv6, DGCTIC, http://www.ipv6.unam.mx/documentos/Tutorial-IPv6-UNAM.pdf

[13] IETF. (2008). *Special-Use IPv6 Addresses.* RFC 5156.

[14] IETF. Prefijo de dirección IPv6 IPv4-compatible. RFCMX3.

[15] IETF. (2003). *Internet Protocol Version 6 (IPv6) Addressing Architecture.* RFC 3513.

[16] IETF. (2004). *6bone (IPv6 Testing Address Allocation) Phaseout.* RFC 3701.

[17] Fernández, A., Gallegos, T. (2012). *Políticas de Ruteo IPv6 en la red CUDI.* CUDI-CDR.

[18] Lazo, C., Fernández, A. (2002). *El protocolo para la nueva era*. IPv6 Forum: Capítulo México.

[19] IETF. (1998). *Generic Packet Tunneling in IPv6 Specification.* RFC 2473.

[20] IPv6 Tunnel through an IPv4 Network, http://www.cisco.com/c/en/us/support/docs/ip/ip-version6/25156ipv6tunnel.html

[21] IEEE. (2008). *Packet by Packet Analysis in Contemporary Network Simulators*. Revista IEEE America Latina.

[22] Dupuy, A., Schwartz, J. y Yemini, Y. (1989). *NEST: A Network Simulation & Prototyping Testbed*. New York: Universidad de Columbia. Recuperado el 30 de octubre de 2013, de http://researcher.watson.ibm.com/researcher/files/us-bacon/Dupuy89NEST.pdf.

[23] Alaettinoglu, C., Dussa, K., Matta, I. y Udaya, A. (1991). *Mars (Maryland Routing Simulator) Version 1.0*. Maryland: Universidad de Maryland, departamento de ciencias de la computación.

[24] http://www.ssfnet.org

[25] http://j-sim.cs.uiuc.edu/

[26] Banks, J., Carson II, J. S., Nelson, B. L. y Nicol, D. M. (2005). *Discrete Event System Simulation*. (4a Ed.). USA: Prentice-Hall.

[27] http://www.isi.edu/nsnam/ns/

[28] http://www.itescam.edu.mx

[29] https://www.netacad.com/web/about-us/cisco-packet-tracer

[30] http://www.opnet.com/university_program/itguru_academic_edition/

[31] http://www.gns3.net/

[32] http://www.gns3.net/dynamips/

[33] http://www.gns3.net/dynagen/

[34] Sportack, M. A. (1999). *IP Routing Fundamentals*. Indianapolis: Cisco Press.

[35] IETF. (1997). *RIPng for IPv6.* RFC 2080.

[36] http://www.labs.lacnic.net/drupal/sites/default/files/ospf-isis-ipv6.pdf

[37] IETF. (2006). *A Border Gateway Protocol 4 (BGP-4).* RFC 4271.