

Emulación de elementos de networking interactuando con máquinas virtuales

Carlos Binker¹, Alejandro Pérez¹, Guillermo Buranits¹, Eliseo Zurdo¹

¹Universidad Nacional de La Matanza, Florencio Varela 1903 (B1754JEC) -- San Justo,
Buenos Aires, Argentina

{cbinker, aperez, gburanits, }@unlam.edu.ar;
ezurdo@alumno.unlam.edu.ar

Abstract. En este trabajo se pretende mostrar la emulación de elementos de networking tales como switches y routers interactuando con máquinas virtuales que emplean sistemas operativos diversos como ser Windows, Mac OS X, Linux en diferentes distribuciones, etc. A tal efecto se emplea una plataforma de software libre denominada GNS3 (Graphical Simulator Network 3). Después de hacer un análisis más pormenorizado de dicha plataforma con sus programas asociados se mostrará un ejemplo de laboratorio en donde se simula una red de una empresa que se conecta con otras dos sucursales mediante enlaces punto a punto, como podría ser el caso de una red de un banco (la casa central con dos sucursales).

Keywords: GNS3, VMware, IOS images, Appliances, Virtual Machine

1 Introducción

En los últimos años el enorme crecimiento registrado en el ámbito del networking, sobre todo teniendo en cuenta el avance vertiginoso de forma exponencial de Internet, ha traído aparejado un importante incremento de las estructuras de hardware. Por esta razón y dada la necesidad de reducir físicamente estas enormes estructuras es que ha nacido un nuevo paradigma denominado *Virtualización* [1]. Clásicamente si por ejemplo se requería montar una granja de servidores, era necesario contar con muchas cajas físicas en donde cada caja constituía un servidor brindando un determinado servicio. Con la virtualización en cambio en una sola caja física se podrían albergar múltiples servidores *lógicos* con la consiguiente disminución de las estructuras de hardware. Pero claro, esto no resulta gratuito, se requieren procesadores con alta potencia de cómputo (varios núcleos para procesamiento paralelo) y mucha capacidad de memoria RAM, como así también gran capacidad de almacenamiento de disco rígido. De esta manera nace el concepto de *Virtual Machine* [2], en castellano máquina virtual, es decir de una estructura lógica que emula los componentes básicos de hardware (disco duro, cpu, ram, placas de red, lector de dvd, audio, video, etc.) y que

corre un determinado sistema operativo. La máquina virtual es en esencia software que utiliza los recursos de hardware de una máquina principal denominada *host*. Cuando se instala una máquina virtual en una máquina *host*, para el usuario ésta se ve como si fuera una máquina física más con las mismas características de una máquina *host*, en donde los recursos a asignar a la máquina virtual son totalmente configurables. La máquina virtual instalada en una máquina *host* se denomina comúnmente *guest*. Por lo tanto, la máquina virtual utiliza un sistema operativo, denominado también *guest* que puede ser Windows, Mac OS X o cualquier distribución de Linux. Existen varias plataformas que permiten crear máquinas virtuales, entre las más populares tenemos *VirtualBox de Oracle* [3], *VMware Workstation* [4], *qemu* [5] (que es nativa en los sistemas Linux), etc. Pero no sólo las computadoras con sus correspondientes sistemas operativos pueden ser virtualizadas, sino que el concepto de virtualización se extiende también a los elementos de *internetworking*, como ser los switches, en donde por citar un ejemplo las *vlans* (Virtual Lans) constituyen switches lógicos que conforman redes LAN independientes que están en una misma estructura física, es decir en un único switch físico. El *GNS3* [6] además de permitir trabajar con los distintos elementos de *networking* y las máquinas virtuales, básicamente computadoras, incorpora un nuevo paradigma que es la posibilidad de incorporar *Appliances* [7]. Un *appliance* consiste en una estructura de hardware que puede emularse a través de una máquina virtual y ser utilizada en una plataforma de simulación, como el *GNS3*, comportándose como si se tratara del equipo físico real, con la consiguiente reducción de costos, ya que en realidad se tiene una virtualización del equipo real, pero que da la apariencia de estar trabajando con el equipo físico real verdadero. Así por ejemplo podemos tener *Appliances* de costosos equipos simulados en esta plataforma y también resulta beneficioso para las empresas porque aumentan sus ventas.

1.1 Ventajas y desventajas de emplear una plataforma *GNS3* frente a la utilización de hardware de red real

Con el *GNS3* podemos emular el comportamiento de una red real utilizando recursos de software (*Appliances*) en vez de los costosos equipos de hardware tal como lo haríamos en forma tradicional. Por lo tanto, algunas de las ventajas que podríamos citar son las siguientes:

- Realizar pruebas de diferentes topologías complejas de red previa a la puesta en producción del equipamiento real.
- Probar actualizaciones y cambios de configuraciones de software en los equipos virtualizados antes de realizarlas en equipos reales y productivos, evitando complicaciones e inconvenientes en la infraestructura real de los clientes.
- Facilitar la enseñanza y el aprendizaje al poder crear laboratorios virtuales idénticos a los entornos reales, permitiendo a los estudiantes reproducir los diferentes escenarios en sus computadoras personales.

Por otro lado, como desventajas de la plataforma *GNS3* podríamos citar las siguientes:

- No se puede probar ni medir la performance de la infraestructura real de red ya que la misma al estar virtualizada presenta una degradación natural con respecto a la estructura original.
- Se requiere de un hardware bastante potente para emular configuraciones complejas de red, esto significa concretamente gran poder de procesamiento y de memoria RAM.

2 Descripción de la plataforma GNS3 y sus programas asociados

El GNS3 es un simulador gráfico de redes que permite emular dispositivos de la línea CISCO. Entre los dispositivos que pueden emularse tenemos routers, switches, firewalls y el mayor valor agregado lo constituye la implementación de máquinas virtuales. En la figura 1 observamos la pantalla principal de trabajo de la plataforma:

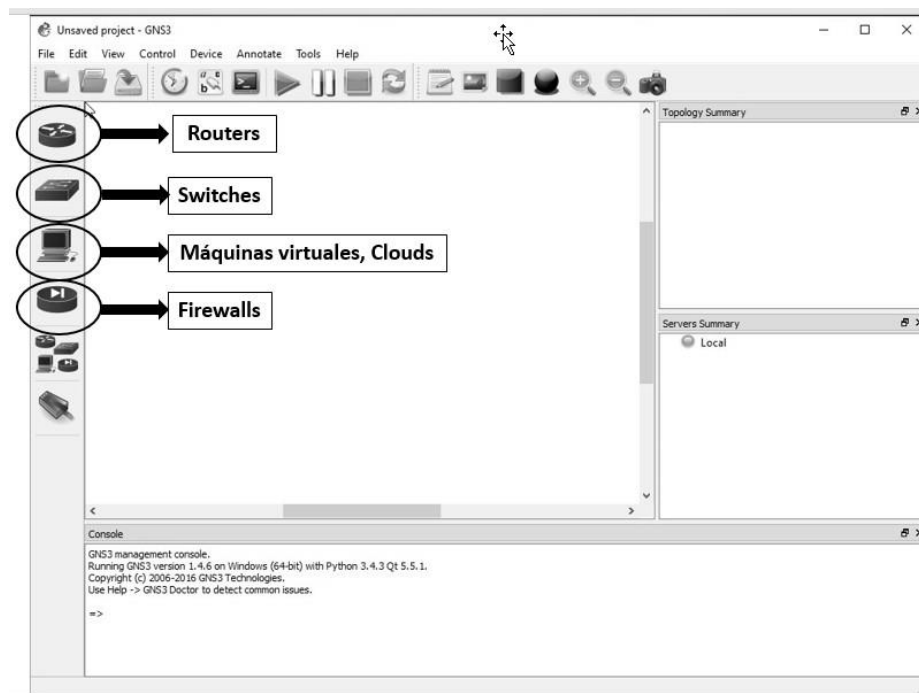


Fig. 1. Pantalla principal de trabajo de la plataforma GNS3

Según la Fig. 1 podemos elegir distintos tipos de routers, switches, máquinas virtuales o Firewalls. Entre los routers, se recomienda el uso de las siguientes plataformas:

c3640, c3660, c3725, c3745, y c7200. El programa asociado a la emulación de los routers CISCO se denomina *Dynamips* [8].

2.1 Configuración

La configuración del GNS3 se lleva a cabo editando las preferencias, en donde se encuentran los siguientes elementos a destacar (ver Fig. 2):

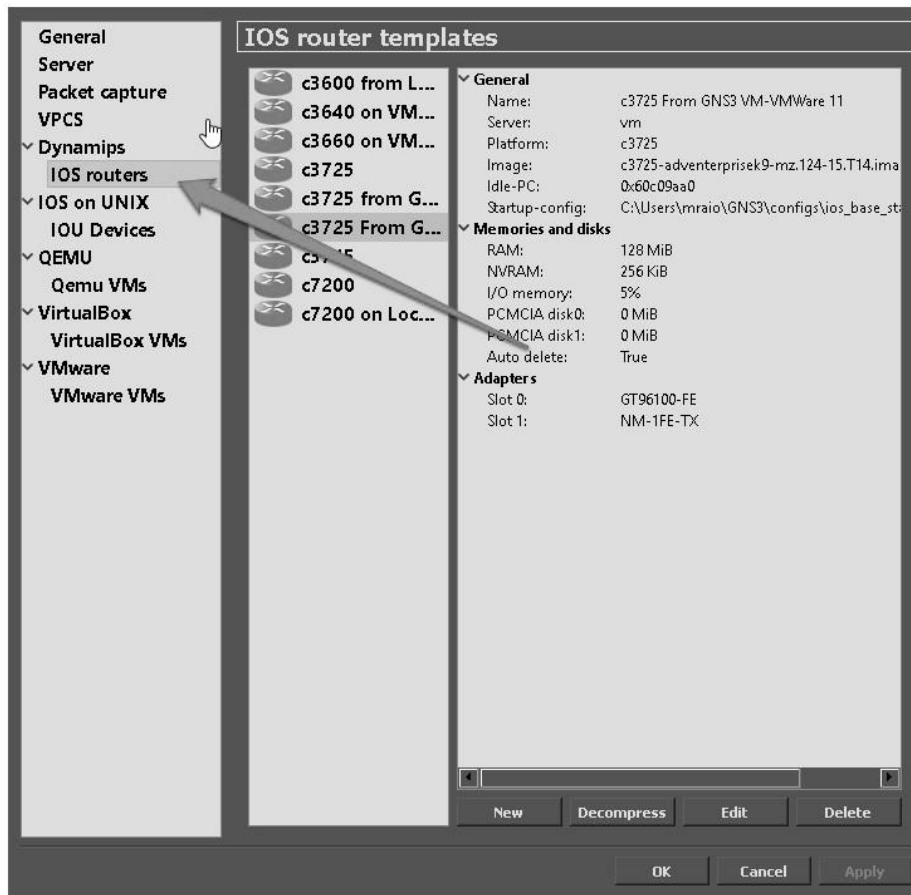


Fig. 2. Configuración de las preferencias de la plataforma GNS3

1. *Server*: en el server se guardará toda la configuración, puede elegirse la opción local, server que emplea la dirección de local host 127.0.0.1 y puerto TCP 8000, GNS3 Virtual Machine server, que emplea una como servidor una máquina virtual que suministra GNS3 o remote server, que permite configurar un servidor externo.

2. *IOS Routers*: desde aquí se selecciona el IOS del router CISCO correspondiente; las posibles plataformas se ven en la Fig.2
3. *Qemu VMs, Virtual Box VMs, VMware VMs*: desde aquí se seleccionan las diferentes máquinas virtuales a emplear en las topologías de red. En el desarrollo experimental que explicaremos más adelante utilizamos VMware Workstation.

3 Diseño de una experiencia de laboratorio empleando GNS3

Se sintetizará mediante el GNS3 la siguiente topología de red:

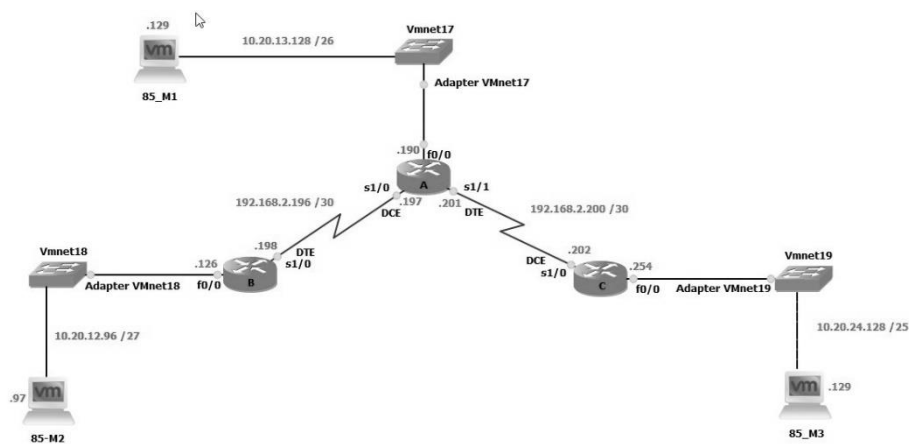


Fig. 3. Topología de red a implementar mediante GNS3

En esta topología tenemos tres routers cisco 3725 (denominados A, B y C). El router A enlaza con los routers B y C mediante un enlace punto a punto simulado a través de una conexión back to back (conexión sincrónica empleando un cable DTE y un DCE en cada extremo del router). Tenemos tres redes LAN y dos redes WAN en la topología. Las direcciones de red y de hosts con sus respectivas máscaras son las siguientes:

LAN A	10.20.13.128 /26	WAN A-B	192.168.2.196 /30
LAN B	10.20.12.96 /27	WAN A-C	192.168.2.200 /30
LAN C	10.20.24.128 /25		

Table 1. Direcciones y máscaras de las redes LAN y WAN de la Fig. 3

Routers	LAN f0/0	WAN s1/0	WAN s1/1
A	10.20.13.190 /26	192.168.2.197 /30	192.168.2.201 /30
B	10.20.12.126 /27	192.168.2.198 /30	
C	10.20.24.254 /25	192.168.2.202 /30	
Máquinas Virtuales	IP host		

85_M1	10.20.13.129 /26
85_M2	10.20.12.97 /27
85_M3	10.20.24.129 /25

Table 2. Direcciones de hosts y máscaras correspondientes a la topología de la Fig. 3

Los switches denominados Vmnet17, Vmnet18 y Vmnet19, corresponden a switches virtuales que utiliza el VMware y su explicación la daremos en el siguiente apartado.

4 Desarrollo de la experiencia

En este apartado se aportará la experiencia de vislumbrar la *interacción* del mundo del networking con las máquinas virtuales. Para ello primero haremos una síntesis preliminar de las herramientas utilizadas y finalmente presentaremos las capturas más relevantes de los resultados obtenidos.

4.1 Herramientas utilizadas

Para la síntesis de la topología de red mencionada con anterioridad emplearemos los siguientes elementos de hardware y software:

- Servidor HP Proliant DL-120 G6 con 12 GB de RAM
- Sistema operativo host Windows 10
- Plataforma de software GNS3 versión 1.5.1
- VMware Workstation 12 Pro version 12.1.1 build-3770994
- Tres routers 3725
- Tres máquinas virtuales con sistema operativo Debian versión 8.5 sin entorno gráfico, denominadas 85_VM1, 85_VM2 y 85_VM3.
- Tres switches virtuales denominados VMnet17, VMnet18 y VMnet 19 aportados por la aplicación VMware Workstation.

Cada router 3725 posee las siguientes placas de hardware:

1. Slot 0: una NM-1FE-TX, identificada como f0/0
2. Slot 1: una NM-4T, identificadas como s1/0, s1/1, s1/2 y s1/3

La configuración de cada máquina virtual es la siguiente:

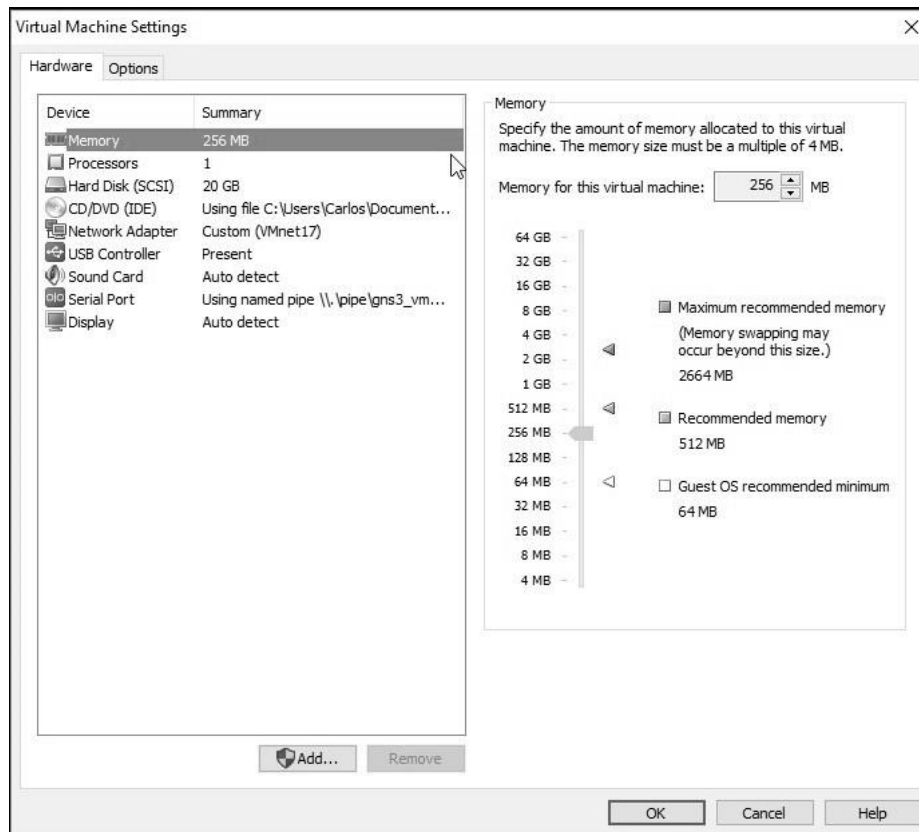


Fig. 4. Configuración de hardware correspondiente a la Máquina Virtual 85_VM1

Observese que se han asignado sólo 256 MB de ram a cada Máquina virtual (no se hace uso del entorno gráfico, ya que no resulta necesario para esta experiencia). Las configuraciones para las máquinas virtuales 85_VM2 y 85VM_3 es idéntica a la de la85_VM1 excepto que ambas máquinas se encuentran conectadas a los switches virtuales VMnet 18 y VMnet 19 respectivamente.

4.2 Configuración de los routers CISCO 3725

En todos los routers se ha configurado RIP versión 2, ya que estamos trabajando con subnetting. A continuación se muestran las tablas de ruteo correspondientes a cada router:

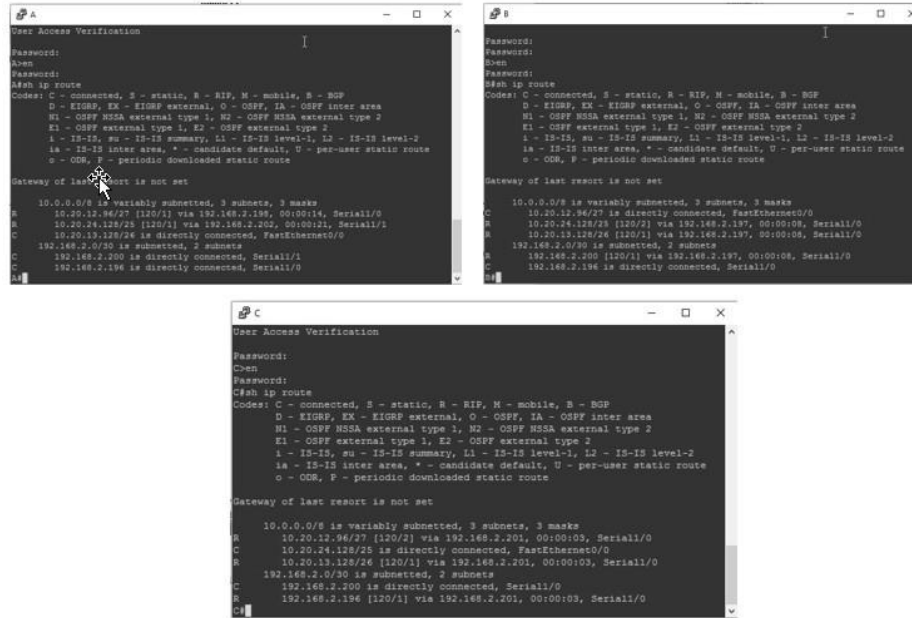


Fig. 5. Tablas de ruteo correspondientes a los routers A, B y C

4.3 Vinculación de los elementos de red con las máquinas virtuales

Para establecer la comunicación entre los dispositivos de red y las máquinas virtuales, en este caso los routers, se debe emplear un *cloud* como elemento auxiliar. En la solapa Ethernet del cloud se elige con qué interface de red se van a vincular los routers con las máquinas virtuales. Como las máquinas virtuales en VMware están asociadas precisamente a los switches denominados VMnet, es que se eligen estas interfaces. Cabe destacar que para que todo esto funcione apropiadamente deberán configurarse las placas de red tanto desde el GNS3, como desde el VMware. A tal efecto el VMware posee un editor de redes que simplifica mucho esta tarea. Con posterioridad, al cloud puede cambiarse el símbolo que lo identifica, siendo en este caso el más apropiado el de un switch.

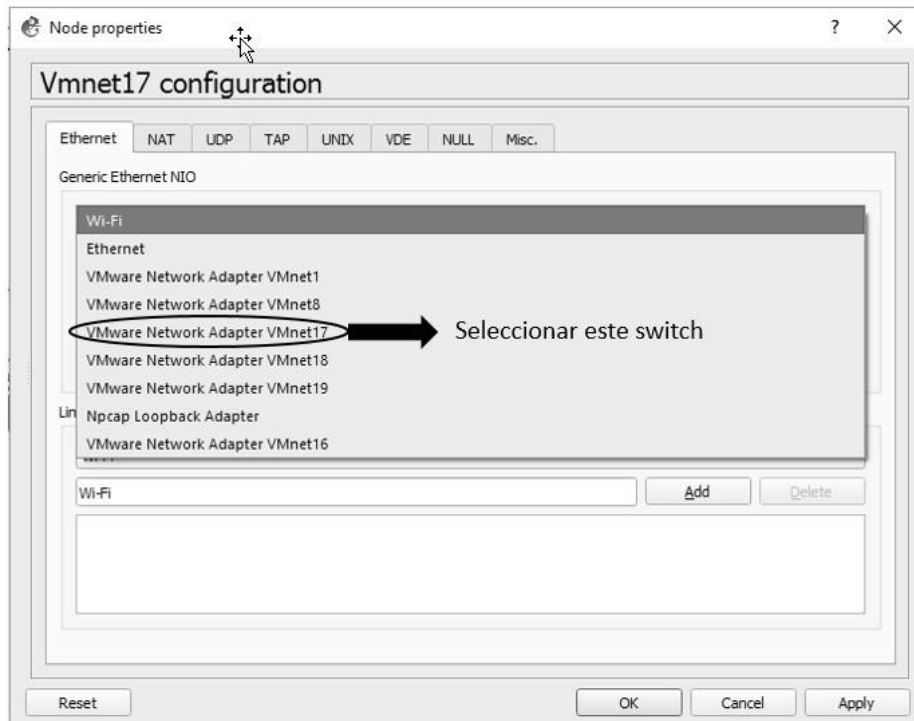


Fig. 6. Configuración del Cloud VMnet17

Idéntica situación deberá realizarse para vincular las dos máquinas restantes 85_VM2 y 85_VM3, es decir hay que crear dos clouds más y asociarlas respectivamente a las interfaces de red vinculadas a los switches VMnet18 y VMnet19 respectivamente.

4.4 Resultados alcanzados

A continuación, mostramos tres capturas realizadas desde cada máquina virtual enviando ping hacia las otras máquinas virtuales. Con esto se corrobora el funcionamiento del laboratorio.

```

root@85_M1:~# ping 10.20.24.129
PING 10.20.24.129 (10.20.24.129) 56(84) bytes of data:
64 bytes from 10.20.24.129: icmp_seq=1 ttl=62 time=45.9 ms
64 bytes from 10.20.24.129: icmp_seq=2 ttl=62 time=57.4 ms
64 bytes from 10.20.24.129: icmp_seq=3 ttl=62 time=67.1 ms
64 bytes from 10.20.24.129: icmp_seq=4 ttl=62 time=69.0 ms
64 bytes from 10.20.24.129: icmp_seq=5 ttl=62 time=66.3 ms
64 bytes from 10.20.24.129: icmp_seq=6 ttl=62 time=63.5 ms
64 bytes from 10.20.24.129: icmp_seq=7 ttl=62 time=63.8 ms
64 bytes from 10.20.24.129: icmp_seq=8 ttl=62 time=49.0 ms
64 bytes from 10.20.24.129: icmp_seq=9 ttl=62 time=69.5 ms
64 bytes from 10.20.24.129: icmp_seq=10 ttl=62 time=69.0 ms
64 bytes from 10.20.24.129: icmp_seq=11 ttl=62 time=85.0 ms
64 bytes from 10.20.24.129: icmp_seq=12 ttl=62 time=70.8 ms
64 bytes from 10.20.24.129: icmp_seq=13 ttl=62 time=70.0 ms
64 bytes from 10.20.24.129: icmp_seq=14 ttl=62 time=53.2 ms
^C
--- 10.20.24.129 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 1314ms
rtt min/avg/max/mdev = 45.946/65.038/85.041/9.745 ms
root@85_M1:~# _

root@85_M2:~# ping 10.20.24.129
PING 10.20.24.129 (10.20.24.129) 56(84) bytes of data:
64 bytes from 10.20.24.129: icmp_seq=1 ttl=61 time=60.4 ms
64 bytes from 10.20.24.129: icmp_seq=2 ttl=61 time=99.5 ms
64 bytes from 10.20.24.129: icmp_seq=3 ttl=61 time=84.7 ms
64 bytes from 10.20.24.129: icmp_seq=4 ttl=61 time=83.3 ms
64 bytes from 10.20.24.129: icmp_seq=5 ttl=61 time=99.0 ms
64 bytes from 10.20.24.129: icmp_seq=6 ttl=61 time=69.4 ms
64 bytes from 10.20.24.129: icmp_seq=7 ttl=61 time=68.8 ms
64 bytes from 10.20.24.129: icmp_seq=8 ttl=61 time=99.3 ms
^C
--- 10.20.24.129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7086ms
rtt min/avg/max/mdev = 60.429/83.108/99.581/14.564 ms
root@85_M2:~#

root@85_M3:~# ping 10.20.13.129
PING 10.20.13.129 (10.20.13.129) 56(84) bytes of data:
64 bytes from 10.20.13.129: icmp_seq=1 ttl=62 time=61.3 ms
64 bytes from 10.20.13.129: icmp_seq=2 ttl=62 time=68.2 ms
64 bytes from 10.20.13.129: icmp_seq=3 ttl=62 time=68.2 ms
64 bytes from 10.20.13.129: icmp_seq=4 ttl=62 time=54.5 ms
64 bytes from 10.20.13.129: icmp_seq=5 ttl=62 time=68.4 ms
64 bytes from 10.20.13.129: icmp_seq=6 ttl=62 time=59.5 ms
64 bytes from 10.20.13.129: icmp_seq=7 ttl=62 time=53.2 ms
64 bytes from 10.20.13.129: icmp_seq=8 ttl=62 time=50.1 ms
^C
--- 10.20.13.129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7067ms
rtt min/avg/max/mdev = 50.193/59.721/68.450/7.259 ms
root@85_M3:~# _
    
```

Fig. 7. Prueba de Ping entre las máquinas virtuales

5 Conclusiones y trabajo futuro

1. A través del GNS3 es posible conectar una estructura virtual de red con redes físicas por medio de los clouds, lo que hace a esta plataforma sumamente potente.
2. Esta es una presentación sencilla en donde se pretende mostrar la enorme performance de este simulador e insistimos se pone el énfasis en la interacción con las máquinas virtuales, que otros simuladores no pueden realizar, como por ejemplo el paquet tracer de CISCO.
3. Se avizora un enorme futuro para la implementación de redes basadas en IPv6.
4. Lo único negativo a destacar es que para hacer un uso fructífero de GNS3 debe tenerse un hardware poderoso y mucha RAM, se aconseja un mínimo de 16 Gb.

6 Referencias

1. Virtualización con VMWare: Manuales USERS (Spanish Edition). Publicación: 20 de enero de 2013 - ISBN: 978-9871857715.
2. Virtualization Essentials 1st Edition. Publicación: 1º mayo 2012. ISBN 13: 978-1118176719
3. <https://www.virtualbox.org>
4. <http://www.vmware.com/mx/products/workstation.html>
5. http://wiki.qemu.org/Main_Page
6. <https://www.gns3.com>
7. <https://www.gns3.com/marketplace/appliances>
8. GNS3 Network Simulation Guide. Publicación: 25 Octubre 2013. ISBN 13: 978-1782160809.