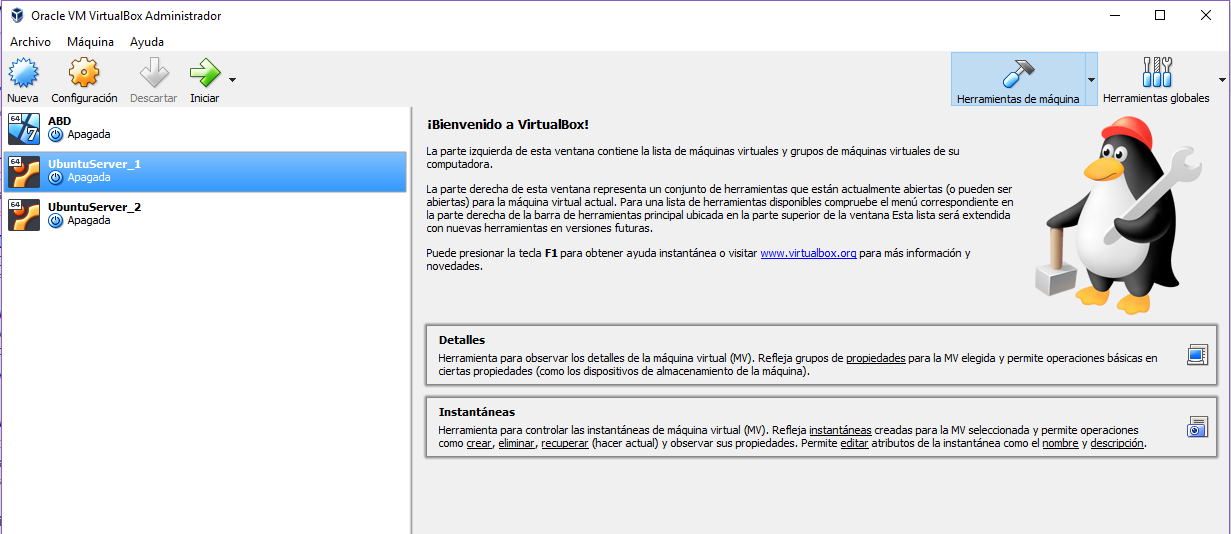
# Instalación del Software necesario

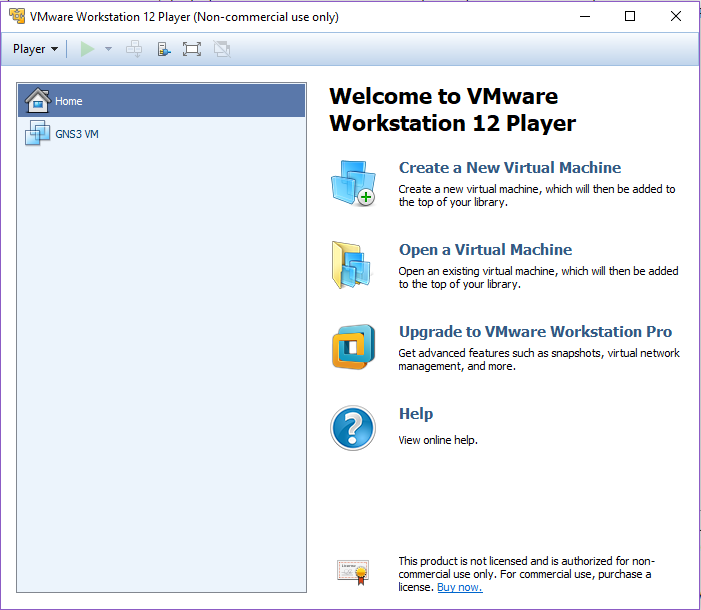
## VirtualBox (versión instalada 5.2.18)

En primer lugar para comenzar con el proyecto se ha instalado el software de virtualización VirtualBox en su versión más reciente a la fecha (5.2.18). Se trata de un programa gratuito desarrollado por Oracle. Gracias a ello podemos ejecutar el sistema operativo Ubuntu Server (en su versión 14.04.4 LTS Server). Podemos cargar estas máquinas más adelante en nuestro proyecto para poder simular elementos de la red. En la instalación inicial se han cargado dos máquinas virtuales de Ubuntu para futuros usos:



## VMWare Workstation 12 player

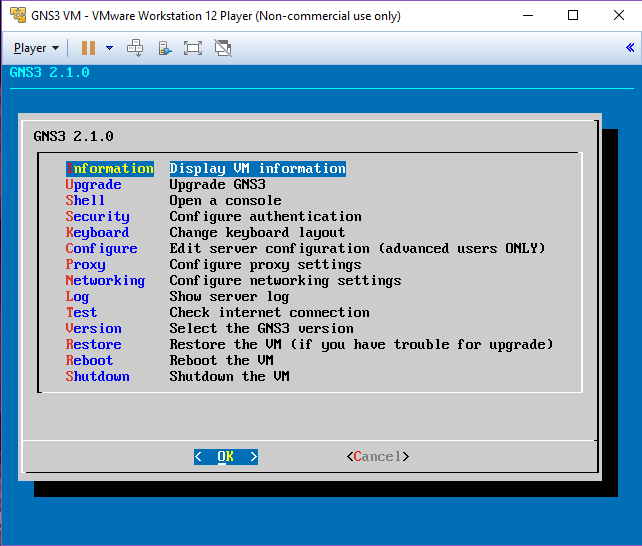
Otro de los software que he necesitado para realizar el proyecto es VMWare en su versión Workstation 12 player (12.5.8). VMWare pertenece a la empresa EMC Corporation (Dell Inc), nos proporciona este software de virtualización totalmente gratis. Una vez instalado vamos a cargar dentro una virtualización del programa que veremos más adelante y en el cual se basa el proyecto: GNS3. Para poder conectar ambos programas deben estar en la misma versión, que es la versión 2.1.0.



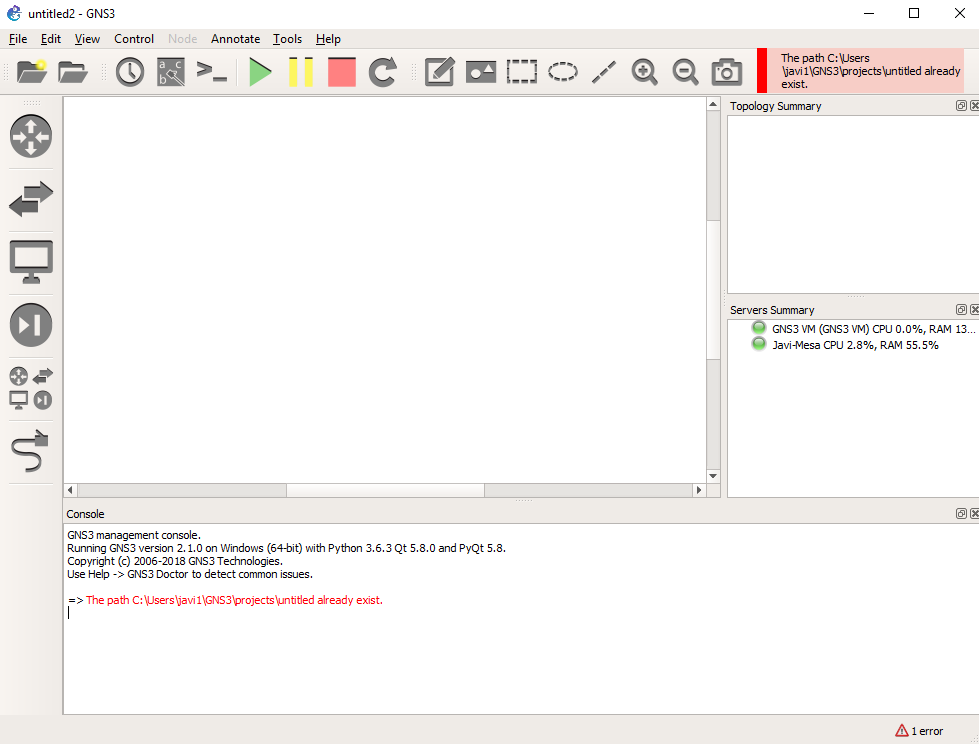
## GNS3 2.1.0

Se trata del programa principal sobre el que se desarrolla este proyecto. Es un software gratuito que permite la simulación gráfica de topologías de red muy complejas y su ejecución. Este programa funciona gracias a Dynamips, se trata de un emulador de sistemas operativos que nos permite ejecutar binarios de Cisco entre otros muchos.

Para su funcionamiento se sincroniza con VMWare y la máquina de GNS3 antes importada sobre este. De esta forma evitamos realizar toda la carga de recursos del programa sobre nuestro propio equipo y lo hacemos sobre el sistema de GNS3 de la máquina virtual. Si se ha realizado correctamente, nada más iniciar GNS3 se nos cargará la maquina de VMWare:



El entorno que nos encontramos nada más abrir el programa será el siguiente:



Como podemos ver en la parte derecha ya podemos escoger el sistema sobre el que trabajar, en primer lugar, vemos el sistema sobre GNS3 de VMWare y en segundo lugar tenemos el equipo local. Ya estamos preparados para comenzar a utilizar el programa.

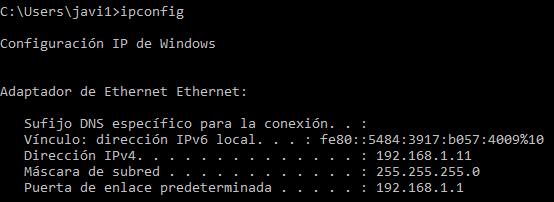
# Uso de Dockers en GNS3

# Conectar GNS3 contra un servidor remoto

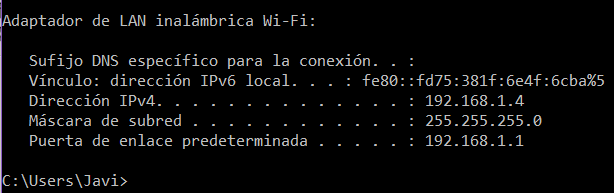
He realizado el proceso de lanzar GNS3 en uno de mis equipos (portátil) contra otro equipo (mesa). Este proceso puede ser muy útil para casos en los que nuestra red empiece a crecer y un equipo carezca de recursos, de esta forma conseguimos que la carga de trabajando sea sobre el servidor y así el equipo en el que estamos trabajando sufra menos de esa carga.

El proceso es sencillo, una vez tenemos la instalación en los dos equipos como hemos visto en los pasos anteriores de instalación, nos fijamos en la IP que tenga cada equipo.

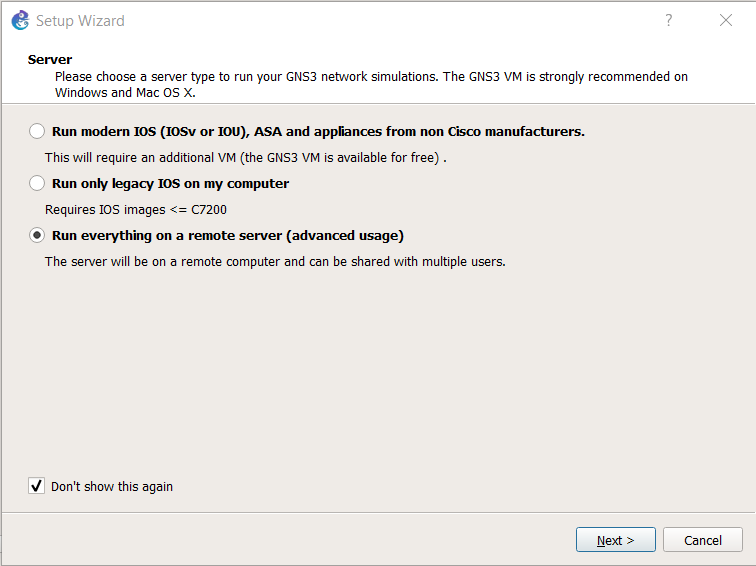
En mi caso en el equipo de mesa (que en este ejemplo hace de servidor):



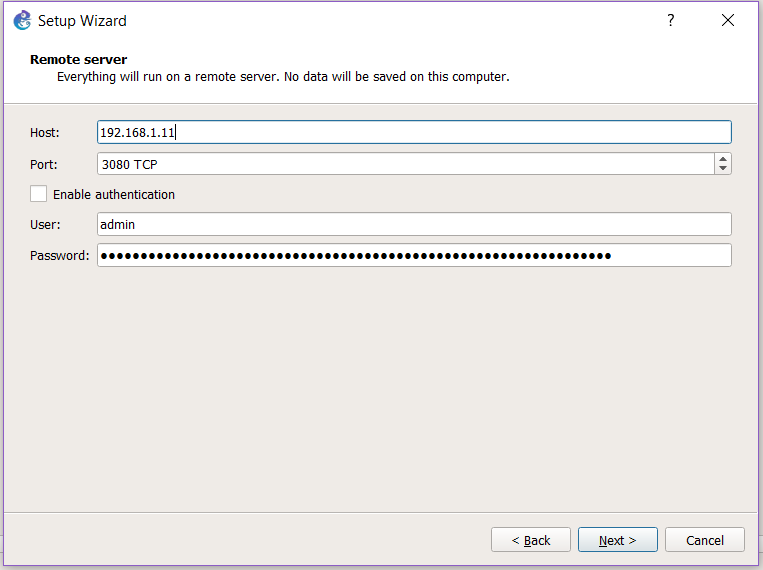
Y en el portátil:



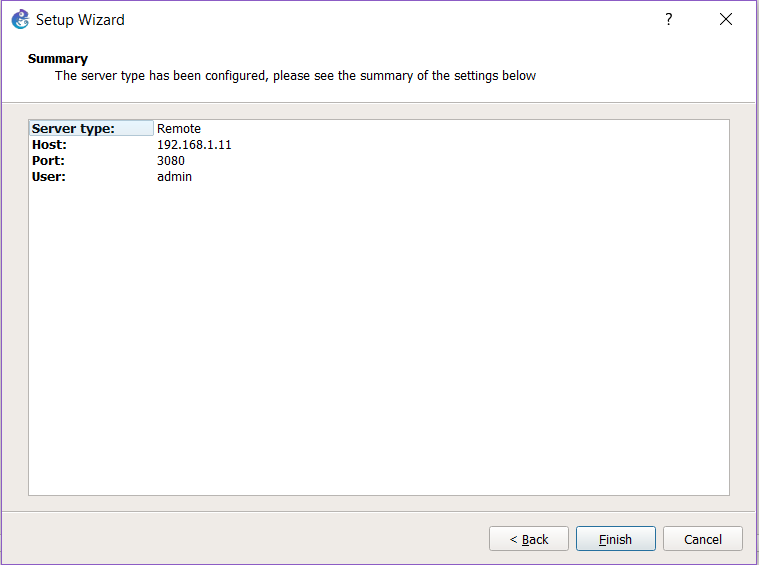
Una vez tenemos claro esto, en la instalación GNS3 del portátil, vamos a cambiar la forma de conectar el programa, desde la opción Setup Wizard:



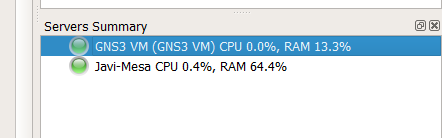
Escogemos la opción de ejecutar sobre servidor remoto, como en la imagen.



Ahora debemos poner la dirección del servidor, para ello hemos buscado la IP de cada equipo, de esta forma ahora podemos introducirla, desmarcamos la opción de autentificación ya que nadie más va a tener acceso y el resto lo dejamos con las opciones por defecto.



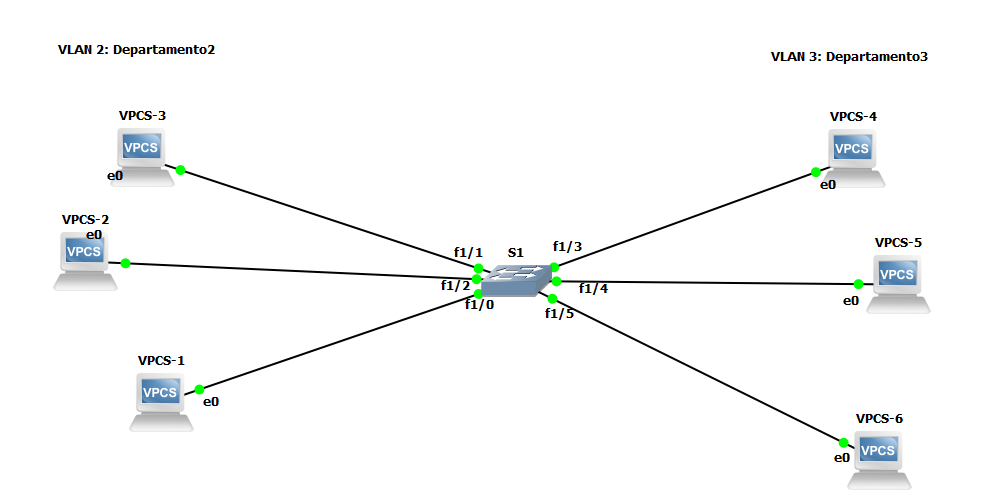
En este último paso ya solo debemos confirmar que esta todo correcto, el programa conectará al servidor y podremos pulsar en finalizar, el resultado es el siguiente:



Ya tenemos configurados nuestros equipos para que se ejecute GNS3 en remoto sobre el servidor.

# Configuración de redes virtuales VLAN.

Para configurar redes virtuales vamos a utilizar un router con funciones de Switch como el que hemos creado en la instalación del programa. Para ello vamos a dividir la red en dos subredes virtuales:



A partir de esta red, empezamos a configurar los equipo, le damos una IP a cada uno coincidiendo con su nombre, el VPCS-1 tendrá la IP 192.168.0.1, el 2 lo mismo pero con la IP 192.168.0.2 y así sucesivamente. Esto lo hacemos mediante el comando:

Ip 192.168.0.x/24

Tras esto pasamos a configurar el Switch, activando todos los puertos a los que se conectan el resto de los equipos, utilizamos para ello:

Configure terminal  
Interface f1/x  
No shutdown

Una vez configurados los equipos y activados los enlaces vamos a crear las VLAN:

configure terminal

VLAN 2  
name Departamento2

Ahora tendremos que asignar a cada puerto la VLAN a la que queramos que pertenezca:

interface f1/x

switchport access vlan 2

interface f1/y

switchport access vlan 3

Vamos a crear una VLAN de administración para poder gestionar el Switch. En primer lugar, vamos a configurar las conexiones telnet para permitir múltiples conexiones:

line vty 0 4

Creamos una contraseña de acceso:

pass 123456

login

Definimos la VLAN para administración y le damos una IP:

vlan 99

name admin

interface vlan 99

ip address 192.168.20.20 255.255.255.0

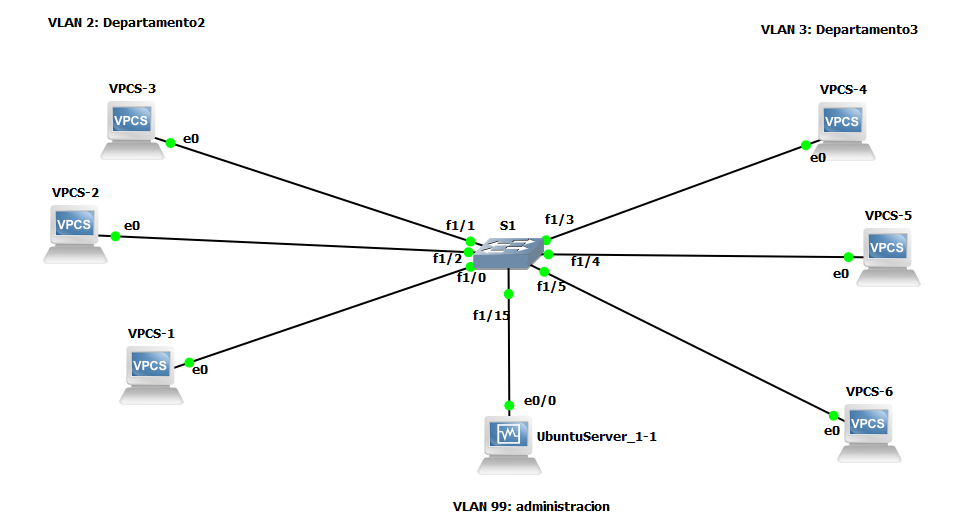
no shutdown

Incluimos la interface que vayamos a utilizar del Switch para administración en la VLAN:

interface FastEthernet1/15

switchport access vlan 99

Una vez tenemos la VLAN de administración lista, vamos a unir a ese puerto un Ubuntu server desde el cual poder conectarnos:



# Servidor Web con apache sobre Ubuntu.

1. Preparación de Ubuntu.

En primer lugar, vamos a configurar un cortafuegos que nos permite bloquear aquellos puertos que no vamos a necesitar, vamos a utilizar UFW. En principio únicamente queremos activarlo para utilizarlo más adelante:

Sudo ufw enable



1. Actualización de Ubuntu.

A continuación, realizo la actualización de Ubuntu con:

Sudo apt update

1. Instalación de Apache.

Tras la actualización, pasamos a la instalación de apache2, para ello vamos a ejecutar el comando:

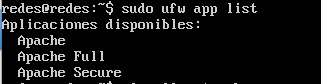
sudo apt install apache2

esto nos pedirá varias confirmaciones y nos permitirá utilizar apache sobre nuestro Ubuntu.

1. Configurar el cortafuegos.

Vamos a ver las aplicaciones que tenemos:

Sudo ufw app list



Permitimos la conexión de apache a través del cortafuegos:

Sudo ufw allow Apache



Y comprobamos el estado del cortafuegos:

Sudo ufw status

