

# Lab 1: Network Device Simulation with GNS3

Rich Macfarlane 2013

## 1.1 Details

**Aim:** The aim of this lab is to begin using the **GNS3 network simulator** and configure Cisco virtual routers. Cisco Routers will be added to a virtual network, and basic networking and security configurations will be performed on the devices.

This will give a foundation to investigate practical network security using virtual network devices within a virtual lab environment in the weeks to come.

## 1.2 Activities

### 1.2.1 (Optional) Install the GNS3 Network Simulator

**GNS3** is a graphical network simulator which can provide simulation/emulation of entire networks, containing many network devices as well as host machines.

To allow realistic Cisco network simulations, GNS3 uses Dynamips; software which enables Cisco device emulation using actual Cisco Operating Systems (OS). This means the virtual devices are running the real Cisco OSs with the full functionality.

GNS can also interface directly with network applications such as Wireshark, as shown in the screen shot below.



The GNS home page can be found at:  
<http://www.gns3.net/>

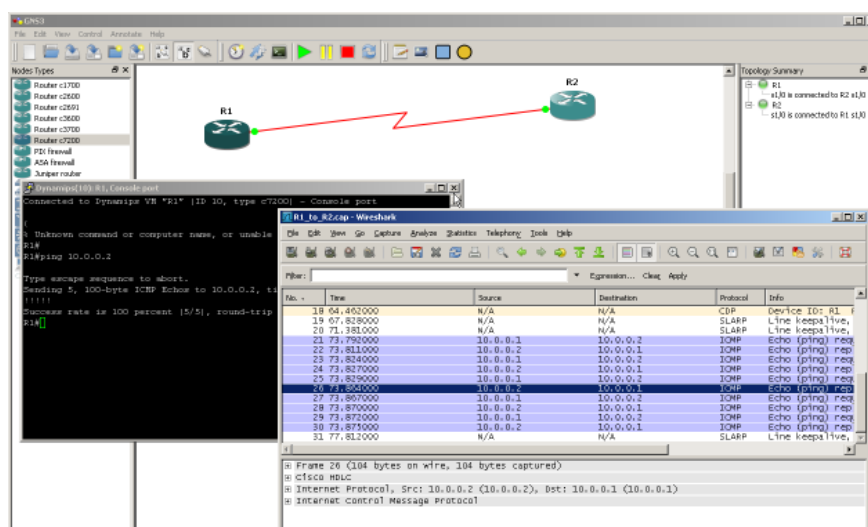


Figure 1 - GNS Graphical Network Simulator

If the GNS3 is not installed on your machine, go to the **GNS3** web page and click the download tab, as shown in the figure below.



Figure 2 - GNS3 Website

Download **GNS3 latest version all-in-one (includes Dynamips, Qemu/Pemu, Putty and WinPCAP)** for **Windows**. GNS3 also runs very well on a Linux system.

Run the Setup executable, and install any of the components which are not already installed.

## 1.2.2 Run and Configure GNS3

To run **GNS3**, from the Windows Start menu type GNS3, or navigate to the executable in Program Files (x86)>GNS3. The first time GNS3 is run, the setup wizard shown below will be displayed. This can be used to perform initial configuration of the simulator.

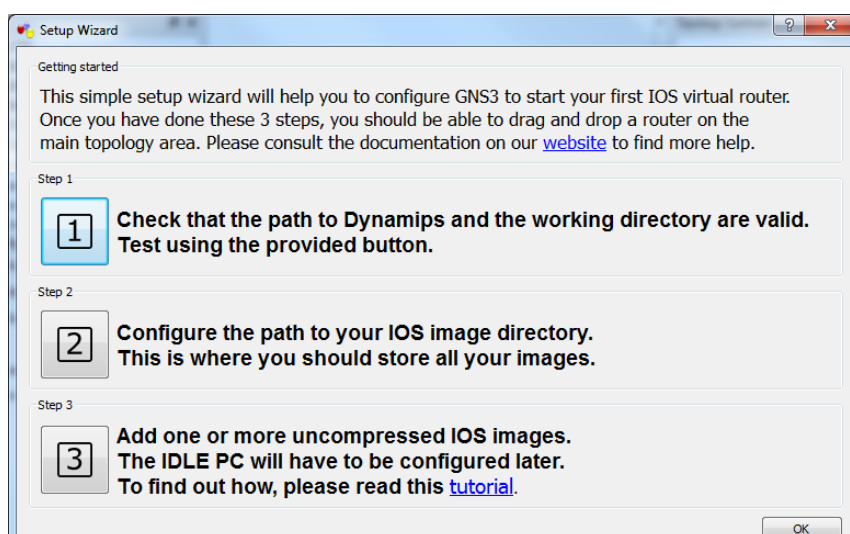


Figure 3 - GNS3 Setup Wizard

## 1.2.3 Step 1 – Setup Dynamips

To configure Dynamips we use the Preferences Dialog>Dynamips Page, shown below. This can also be reached via **Edit>Preferences>Dynamips**.

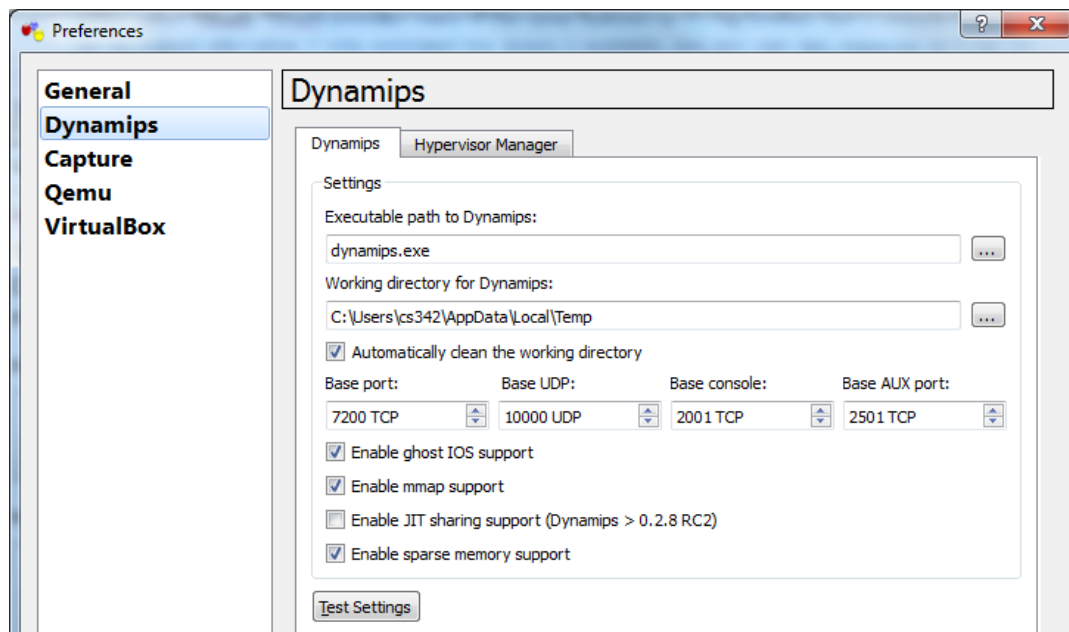
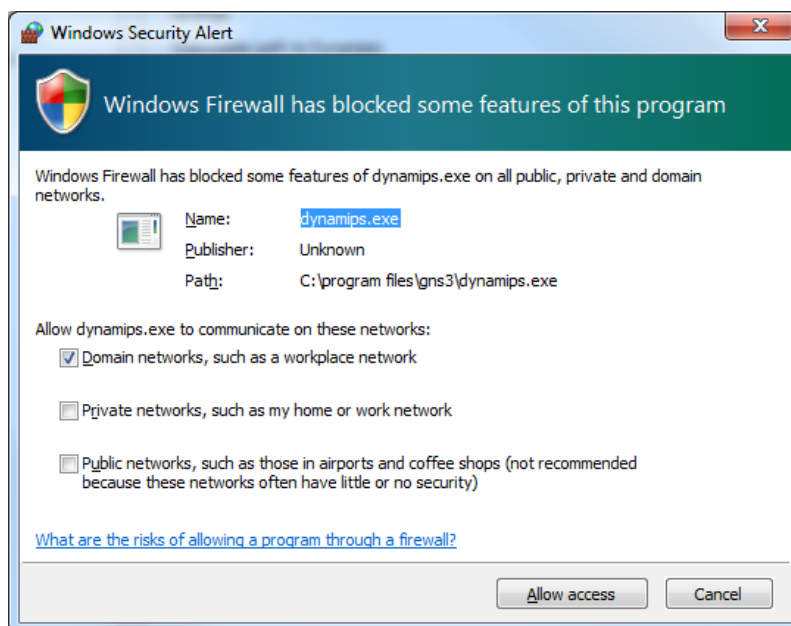


Figure 4 - GNS3 Preferences Configuration

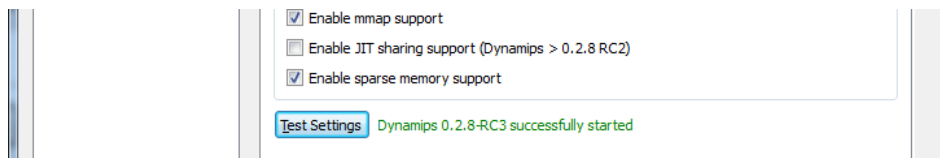
Change the **Working directory for Dynamips** to somewhere on a local drive, which you have permissions to write to, such as **C:\temp**.

Click the **Test Button** (and wait), to check the underlying Dynamips engine is working correctly.

You may need to Allow GNS3 access through the host firewall, as shown below.



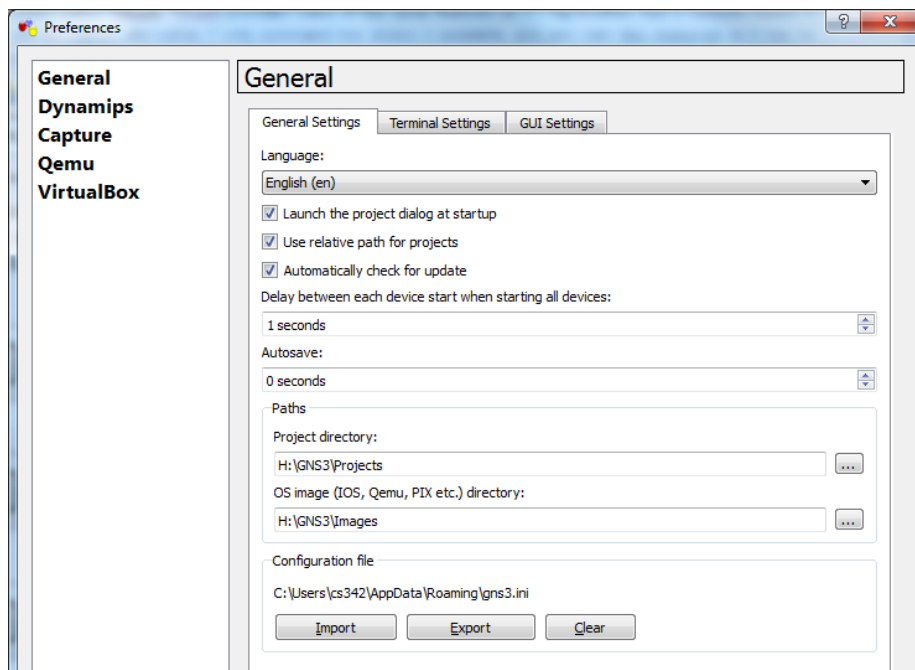
The Dynamips test should be successful, as shown below.




Click the **OK Button** to save the changes.

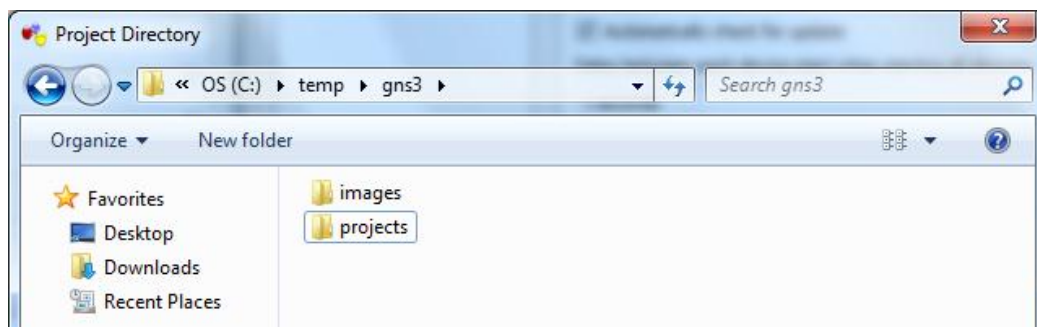
## 1.2.4 Step 2 – Setup Paths to Cisco IOS and Project Directories

To configure paths to IOS files (called **Images** in GNS3), virtual network topology files (called **Projects** in GNS3), and other general settings, use the Preferences Dialog>General Page, shown below. This can also be reached via **Edit>Preferences>General**.



We need to set up the Paths, both for GNS Projects (we will create a new project for each lab), and for the **Cisco Device OS Images**.

Click the **Project directory** button , and create a new folder **Projects**, to save your simulated network topologies in - as shown below. This would typically be under the GNS directory but in the lab use the c:\temp\GNS locations.



**Figure 5 - Projects Directory Creation**

Similarly set up the folder **Images** for the Cisco Network Device OS images we will use for Dynamips device emulation.

Now we have an Images directory we can add a Cisco Router OS to it.

### 1.2.5 Download a Cisco Router Operating System.

We now need to setup a Virtual Router. We need to add a Cisco router Operating System for GNS3 to emulate as a guest OS.



Details of Cisco Networking Devices supported by GNS3 can be found at:  
<http://www.gns3.net/hardware-emulated/>

If network device OSs are not already installed on your system, they can be downloaded to the GNS3 Images directory. Start with a Cisco Router OS from the link below.



The **Cisco 7200 Router OS** can be downloaded from:  
<http://www.dcs.napier.ac.uk/~cs342/CSN11111/c7200-advipservicesk9-mz.124-24.T1.bin>

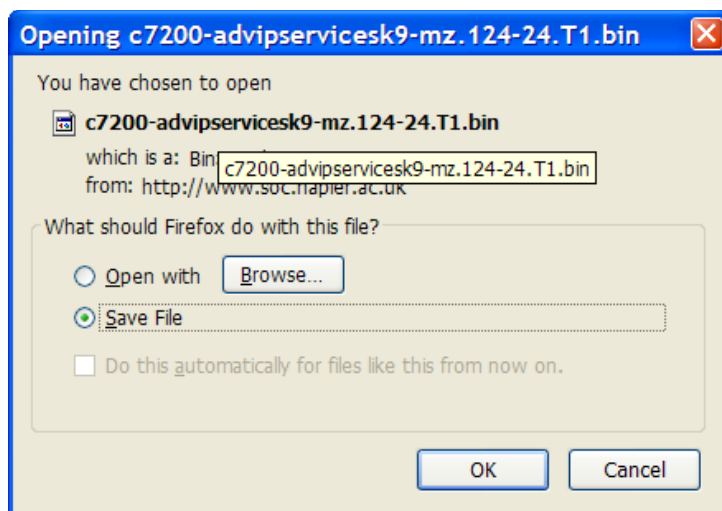


Figure 6 - Download the Cisco Router OS

Save the file in the GNS Images directory you created earlier, such as shown below.

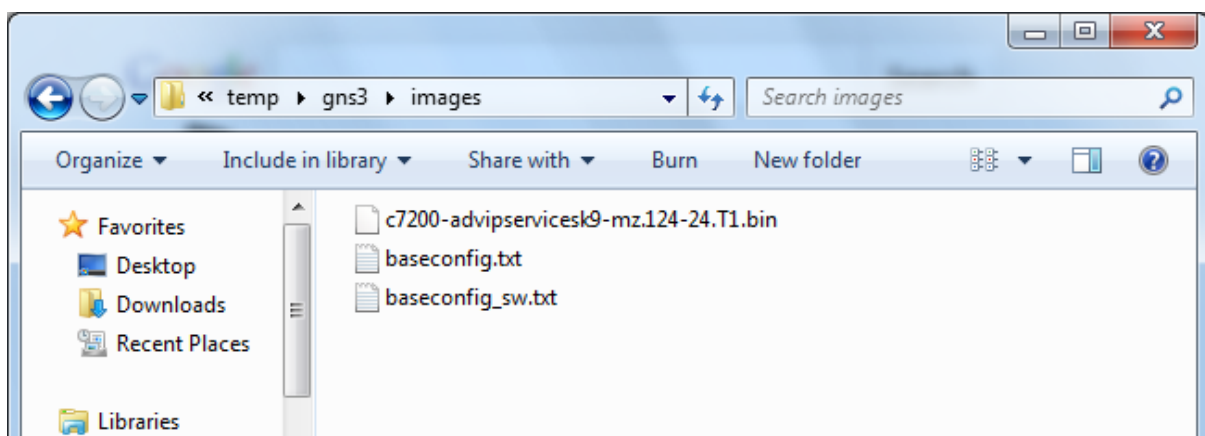
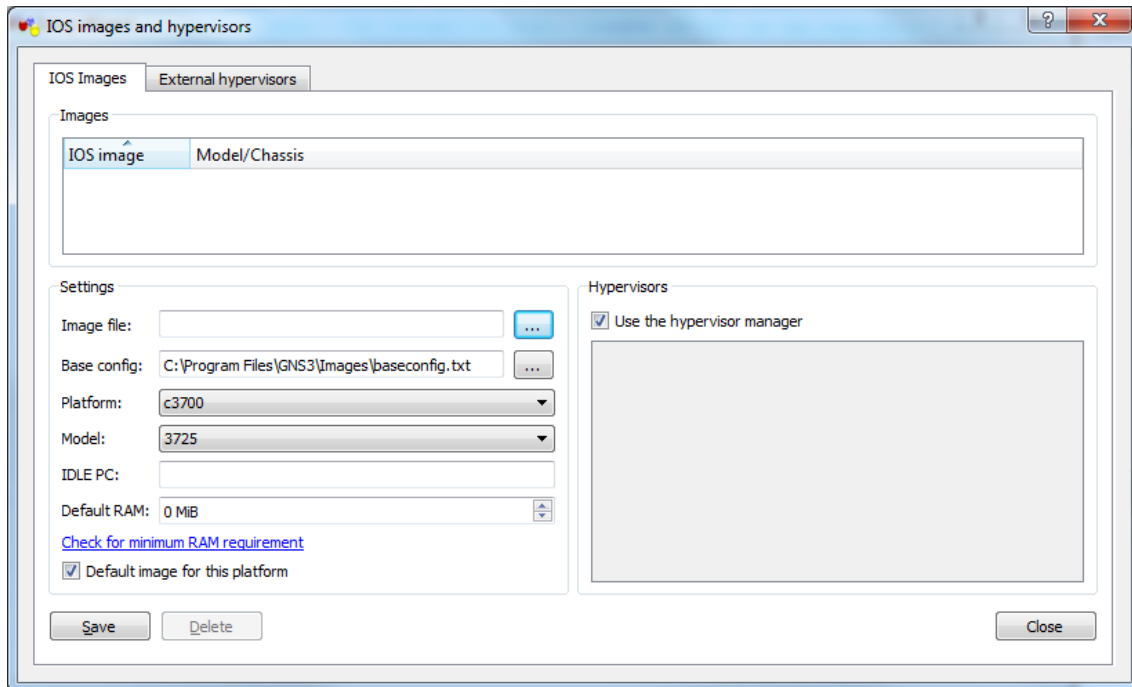



Figure 7 - Cisco Router OS to GNS Images Directory

## 1.2.6 Step 3 - Configure a new Router Type using the Cisco OS

We now need to setup a Virtual Router. We need to add a Cisco router Operating System for GNS3 to emulate as a guest OS.

Go to the IOS Images Dialog, as shown below. This can be reached via **Edit>IOS Images and Hypervisors**.



In **Settings>Platform**, Select the **c7200 Router Platform**. We now need to tell GNS3 to use the downloaded OS to emulate this Router. Click the **Image File** button , and select the downloaded Cisco OS from the Images directory, as shown below.

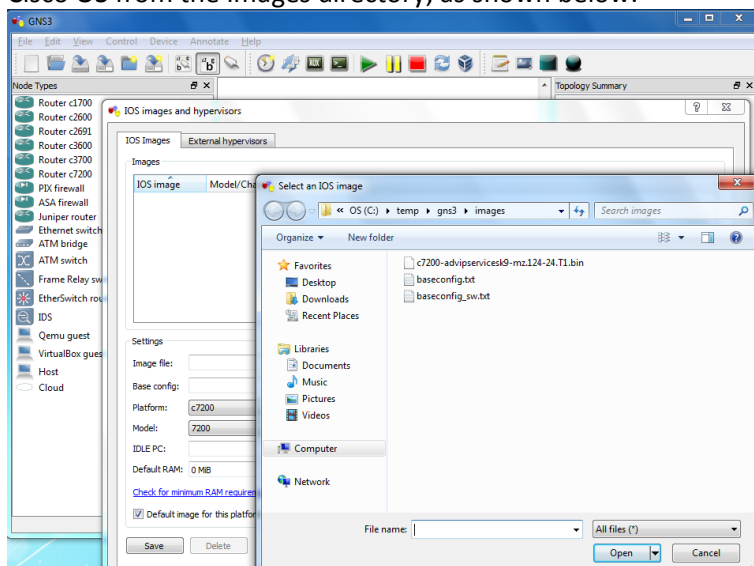


Figure 8 - Select an OS for the 7200 Router Device

Remove the **Base Config** (blank it out), and **Save** the settings, and **Close** the dialog.

Network Security

Network Simulation with GNS3 – Rich Macfarlane 6

## 1.2.7 Using GNS3 to Configure a Virtual Router

Add a virtual 7200 Router to the network, by dragging from the **Node Types** panel to the network topology panel, as shown below Figure 9.

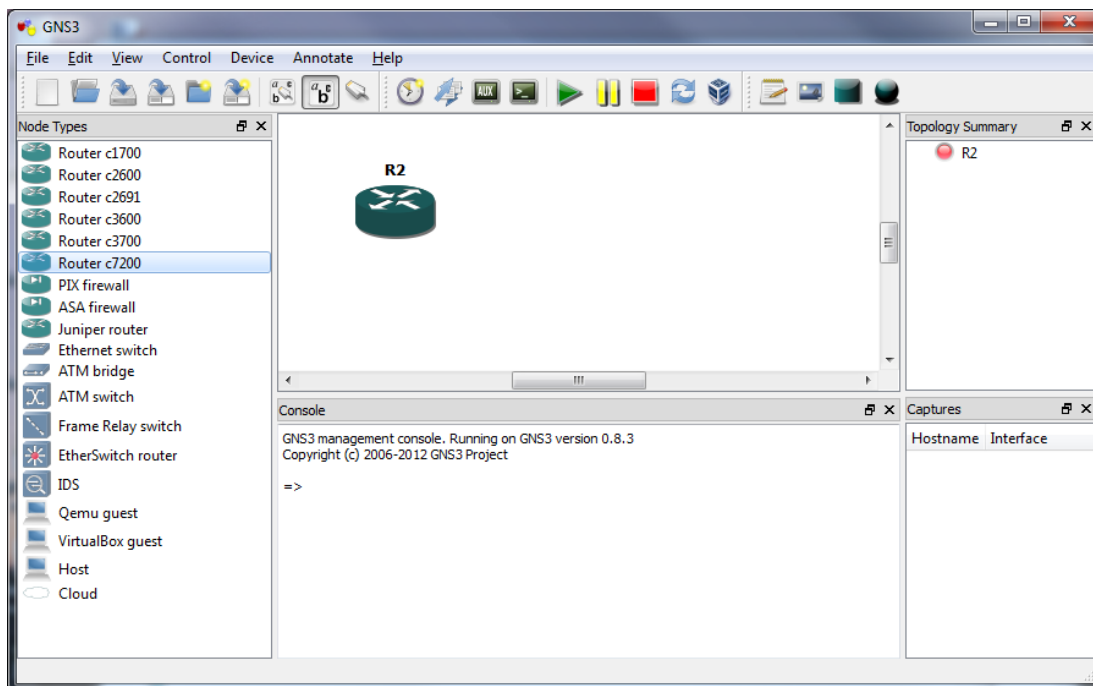


Figure 9 - Adding a Router to the network

### Configure Virtual Router

To configure the virtual router, on the router icon use **Right Click>Configure**, or double click the Router we want to configure. This shows the Node configuration dialog shown below.

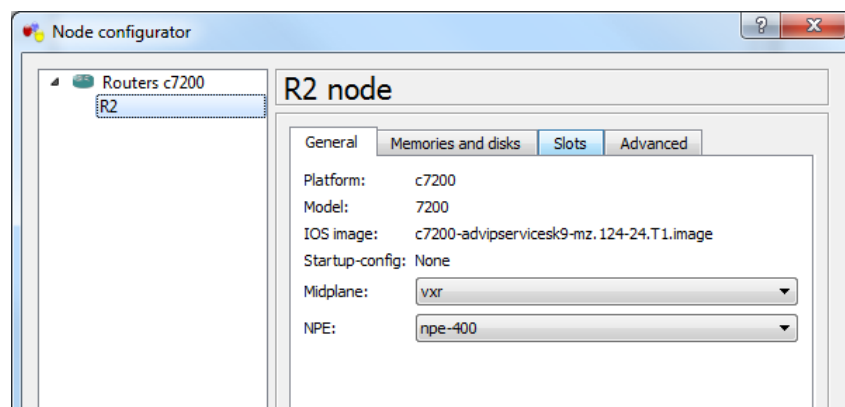


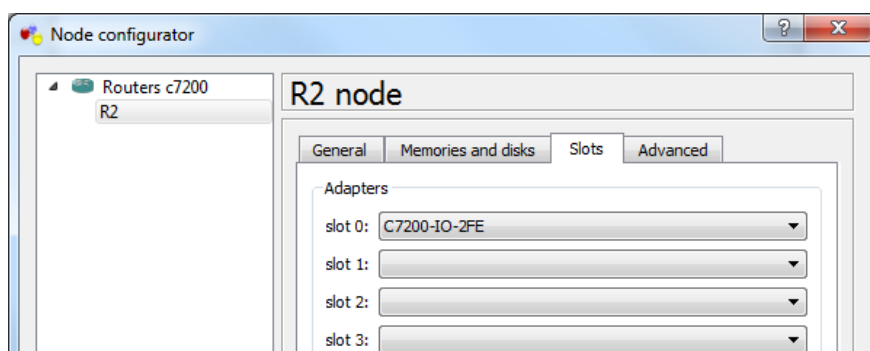
Figure 10 - Configure the Routers Interfaces

### Configure Network Interfaces

The Cisco 7200 router, by default has empty network interface slots, and we need to add some adapters to the slots before we can use the routers networking capabilities. Images below show a router, and some of the empty slots which can be filled with network interface cards, and a “FE Interface Adapter.



Select the **Slots** tab and a double **Fast Ethernet 2FE** Interface Adapter to the virtual router as shown below. This has 2 Fast Ethernet interfaces as shown above on the right.



This window simulates the adding/removal of network interface modules on a physical router. Compare the available modules, with the modules on the physical Cisco routers in the labs if you have access, or google for router/interface adapter details.

## 1.2.8 Boot the Virtual Router

Boot the Router, with **Right Click>Start**. Open a console Window with **Right Click>Console**, and watch the router boot up, as shown below. Press the **Enter** key until there is a response from the router.



```

R2

PCI bus mb2 (Slots 2, 4, 6) has a capacity of 600 bandwidth points.
Current configuration on bus mb2 has a total of 0 bandwidth points
This configuration is within the PCI bus capacity and is supported.

Please refer to the following document "Cisco 7200 Series Port Adaptor
Hardware Configuration Guidelines" on Cisco.com <http://www.cisco.com>
for c7200 bandwidth points oversubscription and usage guidelines.

2 FastEthernet interfaces
125K bytes of NVRAM.
Installed image archive

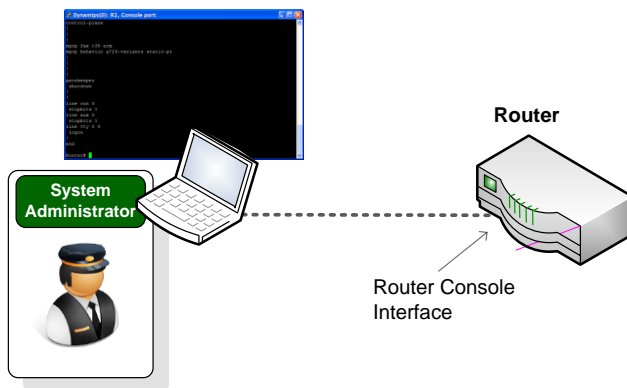
65536K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
SETUP: new interface FastEthernet0/0 placed in "shutdown" state
SETUP: new interface FastEthernet0/1 placed in "shutdown" state
% Crashinfo may not be recovered at bootflash:crashinfo
% This file system device reports an error

Press RETURN to get started!

```

Figure 11 - Console Window - Router Booting

This console window simulates an administrator physically connecting to the router with a laptop, via the routers console port, and using a command line to configure, as illustrated below. This Command Line Interface (CLI) allows the configuration of the router using the Cisco IOS Command language.



If the router terminal is in the configuration mode, as shown below, exit by typing **no**

```

Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>

```

```
2 FastEthernet interfaces
125K bytes of NVRAM.
Installed image archive

65536K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).

--- System Configuration Dialog ---

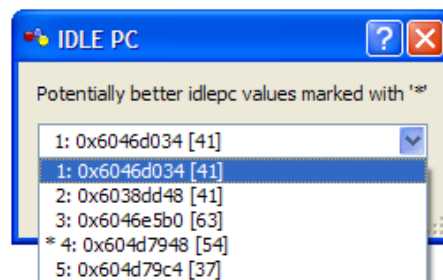
Would you like to enter the initial configuration dialog? [yes/no]: {
```

## 1.2.9 Host System Performance Monitoring

Before doing any configuration it is extremely important to monitor the performance of the host system running the GNS3, and configure the resource use of virtual devices. This is done by configuring the **idlepc value** for the device type being used. It prevents the Cisco OSs consuming all of the host machines resources.

Run the Windows Task Manager using CTRL+SHIFT+ESC to monitor the hosts resource usage.

Configure the idelpc for the virtual router by **Right click on the Router>Idle PC**. Select a preferred value which should be highlighted with an \*, as shown below.



You should notice a drop in CPU usage immediately. If not try another idelpc value.



**Note:** Setting the idelpc value for the IOS we are using is a very important step. When a Cisco IOS is running, it can consume up to 100% of the CPU. This will cause the system to become sluggish and will prevent building more complex topologies. However, if an idelpc value is set CPU usage is reduced dramatically. The IOS is put into a sleep state when it is not in use and is woken only when it is necessary.

## 1.2.10 Basic Cisco Router Configuration

The router can now be configured using the console, the Command Line Interface (CLI). Its important to gain a good understanding of the basics of Cisco device configuration via the CLI, as this will be the foundation for most of the labs in the module.

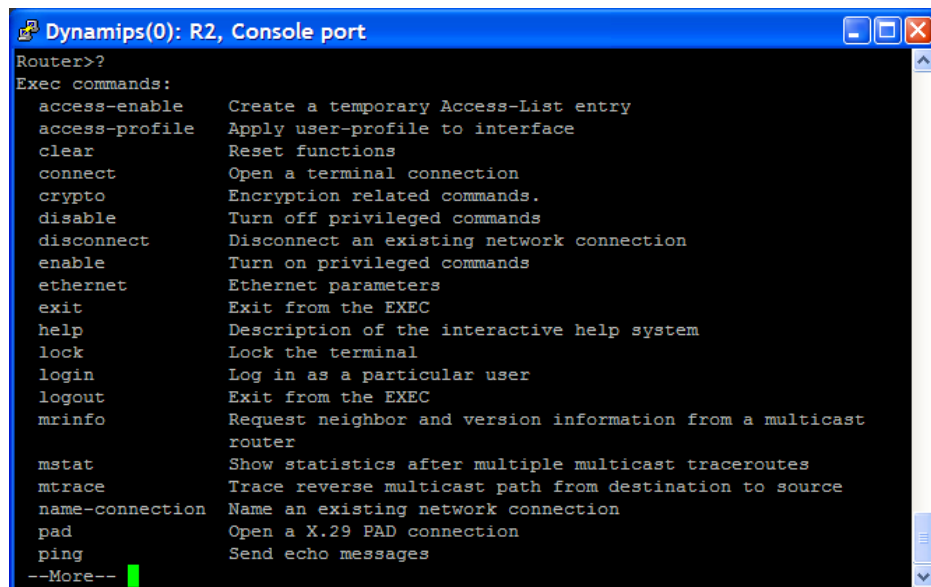


To assist with the cisco router configuration commands the following can be used:  
<http://www.cisco.com/en/US/docs/ios/preface/usingios.html>

Cisco router CLI has many different **Command Modes**, each giving access to a range of commands. When the router boots, the command line is in **User Exec Command Mode**, with the **Router>** prompt.

If the router prompt is **Router#** and not **Router>**, use the **disable** command until the prompt is **Router>**.

Only a limited set of commands are available in this mode. Type **?** to see the available commands for the current command mode. The figure below shows the commands being listed for user exec mode.



```
Router>?
Exec commands:
access-enable      Create a temporary Access-List entry
access-profile     Apply user-profile to interface
clear              Reset functions
connect            Open a terminal connection
crypto             Encryption related commands.
disable            Turn off privileged commands
disconnect         Disconnect an existing network connection
enable             Turn on privileged commands
ethernet           Ethernet parameters
exit              Exit from the EXEC
help              Description of the interactive help system
lock              Lock the terminal
login             Log in as a particular user
logout            Exit from the EXEC
minfo             Request neighbor and version information from a multicast
                  router
mstat             Show statistics after multiple multicast traceroutes
mtrace            Trace reverse multicast path from destination to source
name-connection   Name an existing network connection
pad               Open a X.29 PAD connection
ping              Send echo messages
--More--
```

Figure 12 - User Exec Mode Commands

Try the **show running-config** command. An error should be generated, as this mode does not have permissions for the command.

### Privileged Exec Command Mode

From the user exec mode, enter Enable Command Mode, more commonly known as **Privileged Exec Command Mode** using the **enable** command as shown below. A **Router#** prompt is now shown, and more privileged commands are now available.

```
Router> enable
Router#
```

View the available commands using **?** and scroll back up the console window to compare the command sets.

### Questions

Q: Are there more or less commands available in **Privileged Exec Command Mode**?

View the routers configuration file with the command **show running-config**. It should be similar to the figure below with no IP Addresses or Passwords set up. <SPACE> and <RETURN> can be used to scroll page or line at a time. A full default configuration for a Cisco router is shown in **Appendix 1**.

The following shows Router Command modes with the commands to navigate between them. The associated prompts are shown on the bottom right.

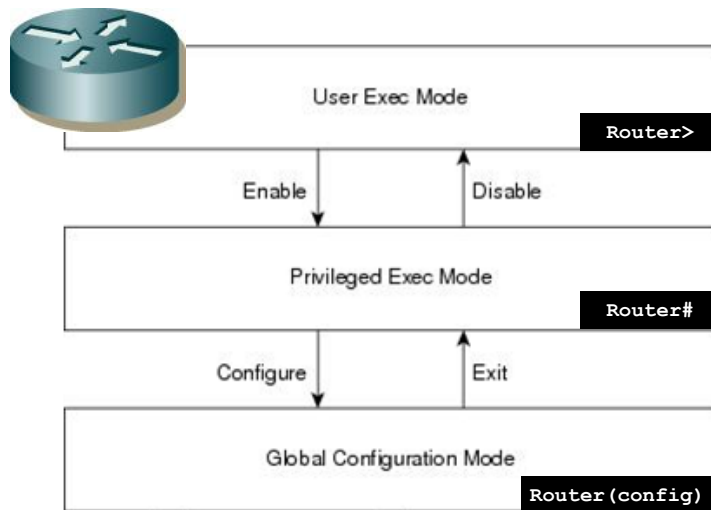


Figure 13 - Router IOS Command Modes



**Completing Partial Commands** Parts of commands can be completed, as in Linux, using the TAB key with a unique partial command. Try the command **show run <TAB>**. The command should be automatically completed.

```
Dynamips(0): R2, Console port

Current configuration : 829 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
ip cef
!
!
!
!
--More--
```

### Global Configuration Command Mode

From the privileged exec mode, enter **Global Configuration Mode**:

```
Router# configure terminal
Router(config)#
```

From this command mode, Router configuration changes can be made. Change the device hostname to Router1:

```
Router(config)# hostname Router17
Router17(config)#
```

Note the prompt has now changed to show the new router name.

#### Questions

Q: Does the Routers name in GNS change when we change the hostname?

If you want to remove a configuration command from the router, simply negate the command by using the **no** command in from of any command. For example:

```
Router17(config)# no hostname Router17
Router(config)#
```

To move from a higher command mode to a lower mode, use the **exit** command or CTRL+C, and to move from Priv Exec to User Exec use **disable**:

```
Router# config terminal
Router(config)# exit
Router# disable
Router>
```

## 1.2.11 Basic Router Security/Device Hardening

### Configure a Password for access to Privileged Exec Command Mode

Cisco IOS supports two commands that set access to the privileged exec mode. The historical command, **enable password**, uses weak cryptography to secure the password, and should never be used if a more secure method is available.

The **enable secret** command uses a one way MD5 cryptographic hash algorithm to store the password. Hash algorithms will be discussed in more detail in a later Cryptography unit.

Password security relies not only on the cryptographic algorithm used, but also the password selected. Weak, easy to remember password will be used in the labs, but longer, more complex passwords should always be used in production environments.

Set the privileged exec password to **cisco**.

```
Router1#config t
Router1(config)# enable secret cisco
```

The enable password is now set to **cisco**. The result of this can be seen by doing the following:

```
Router1(config)# exit
Router1# disable
```

```
Router1> enable
Password: cisco
```

Router1#

#### Questions

Q: Why would setting a password on the privileged mode be a good idea?

View the routers configuration file again, using the **show run** command, from the appropriate command mode.

#### Questions

Q: What are the last 5 characters of the privileged command mode password?

Try setting the privileged exec password a second time to the same value: **cisco**.

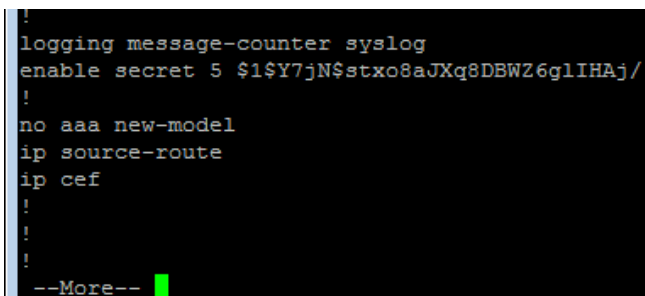
```
Router1# config t  
Router1(config)# enable secret cisco
```

View the routers configuration file again, using the **show run** command, from the appropriate command mode.

#### Questions

Q: What security are the last 5 characters of the privileged command mode password?

Q: Is this the same encrypted password?



```
!  
logging message-counter syslog  
enable secret 5 $1$Y7jN$stxo8aJXq8DBWZ6glIHAj/  
!  
no aaa new-model  
ip source-route  
ip cef  
!  
!  
!  
--More--
```

The encrypted password is shown in the configuration details for the router which can be a problem if configurations are printed. The **secret 5** shows it is a MD5 hash of the plaintext password.

To make things more secure the MD5 hash is salted. This means the same password gives a different hash output every time, and is harder to crack. The salt value is shown between the 2<sup>nd</sup> and 3<sup>rd</sup> \$ character.

### 1.2.12 Configure Banner Message

Banners can be displayed to users trying to gain administrative access to a network device. The Cisco Message of the Day (MOTD) banner, which is displayed at login, is commonly used to greet the user.

This can have legal and security implications for an organisation. For example, a welcome message should never be displayed, as this could be seen as an invitation to unauthorised users to try access the device.

A banner should include information about authorization, penalties for unauthorized access, connection logging, and applicable local laws. An organisations **security policy** should provide policy on banner messages.

To configure a banner use the following command in **Global Configuration Mode**:

```
Router(config)# banner motd [delimited char] <message> [delimited char]
```

Try something similar to the following:

```
Router> enable
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)# banner motd #
Enter TEXT message.  End with the character '#'
*****
*                                     *
*               WARNING               *
*   YOU HAVE ACCESSED A RESTRICTED DEVICE   *
*   USE OF THIS DEVICE WHITHOUT PRIOR AUTHORISATION *
*           IS PROHIBITED, AND WILL BE PROSECUTED *
*           ALL CONNECTIONS ARE LOGGED *
*                                     *
*****
#
Router1(config)# exit
Router1#
```

#### Questions

Q: Why would details about the organisation, the network, or the device being logged into be a bad idea in a banner message?

Q: What would be the global configuration command to *remove* the MOTD banner?

## 1.2.13 Router Network Interface Configuration

### Configure the Routers Fast Ethernet Network Adapter

To view the routers network interfaces and their current states, use the **show ip interface** command, from Priv Exec command mode, as shown below.

```
R1# show ip interface brief
```

#### Questions

Q: What are the routers interface names?

Q: What are the assigned IP Address?

Q: What is its current status of the interfaces?

The network adapter, we added to the router earlier has to be assigned a network layer address, or **IP Address**, to be able to communicate with other devices.

```
Router1(config)# interface fa0/0
Router1(config-if)# description TO THE LAN 192.168.100.x NETWORK
Router1(config-if)# ip address 192.168.100.1 255.255.255.0
```

The no shutdown command, is needed to enable the interface for communication

```
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1#
```

Watch as the interface becomes active:

```
*Sep 14 10:41:13.843: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
```

Check the devices network interfaces and their current states again.

#### Questions

Q: Does the interface have an IP Address, and what is the current state now?

Q: Why did we configure the administration security before the interfaces?



## 1.2.14 Optional Challenge – Extend Topology

### Add and Configure a 2<sup>nd</sup> Router

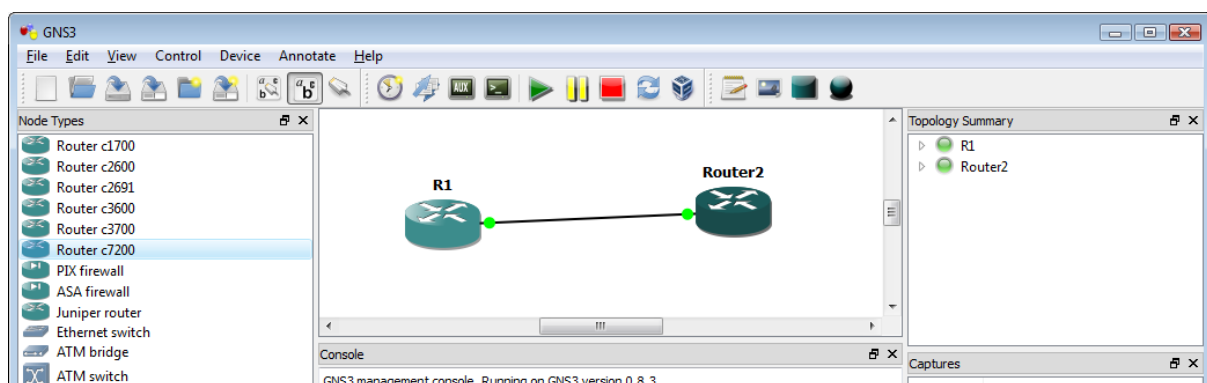
Add another router to the topology, and add a 2FE network interface adaptor.

Start the router, and start a CLI terminal. Check the host machine resource usage and set idelpc is necessary.

Set the hostname **Router2**. Assign its interface the IP Address **192.168.100.2**

```
Router2(config)# interface fa0/0
Router2(config-if)# description LAN TO THE 192.168.100.x NETWORK
Router2(config-if)# ip address 192.168.100.2 255.255.255.0
```

Cable a link between the 2 network interfaces, using the  button, selecting **manual**



### Test Connectivity

From the first Router use the **ping** command to test connectivity between the interfaces. The ping command uses ICMP packets and can be used to check if a device/interface exists, and is responding.

```
Router1(config)# ping 192.168.100.2
```

Router2 should be able to ping Router1s interface

```
Router2(config-if)#do ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!.!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 28/49/72 ms
Router2(config-if)#
```

### Questions

Q: How might the ping command be misused?

Q: Try to ping google.com, and then amazon.com

## 1.3 Appendix 1 - default Cisco IOS router configuration

---

```
Current configuration : 824 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/1/0
no ip address
shutdown
no fair-queue
!
interface Serial0/1/1
no ip address
shutdown
clock rate 2000000
!
interface Vlan1
no ip address
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
login
!
scheduler allocate 20000 1000
end
```