Centre de la Imatge i la Tecnologia Multimèdia (CITM)

Grau en Multimèdia

Laboratori de Arquitectura i Seguretat en Xarxes Informàtiques

Davide Careglio

Septiembre 2019

Índex

Entorno del laboratorio

En este capitulo se introduce el entorno de las actividades practicas y en concreto se describe la herramienta Cisco Packet Tracer Student versión 6.2 que se usará (https://en.wikipedia.org/wiki/Packet_Tracer). Se usará esta herramienta en la mayoría de las actividades prácticas.

Introducción al Packet Tracer Student

Packet Tracer es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red y resolver preguntas del tipo "qué pasaría si...". Como parte integral de la Academia de Networking de Cisco, Packet Tracer provee capacidades de simulación, visualización, evaluación y colaboración y facilita la enseñanza y aprendizaje de conceptos básicos de redes.

Esta herramienta permite crear redes fácilmente en un entorno grafico. La versión actual de Packet Tracer soporta un conjunto de protocolos simulados, al igual que enrutamiento básico con RIP, OSPF, y EIGRP. Aunque Packet Tracer provee una simulación de redes funcionales, utiliza solo un pequeño número de características encontradas en el hardware real corriendo una versión actual del Cisco IOS. Packet Tracer no es adecuado para redes en producción.

La Figura 1 muestra la aplicación. En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego haciendo clic sobre ellos se puede entrar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco IOS. Una vez completada la configuración física y lógica de la red, también se pueden hacer simulaciones de conectividad (pings, traceroutes) todo ello desde las mismas consolas incluidas.

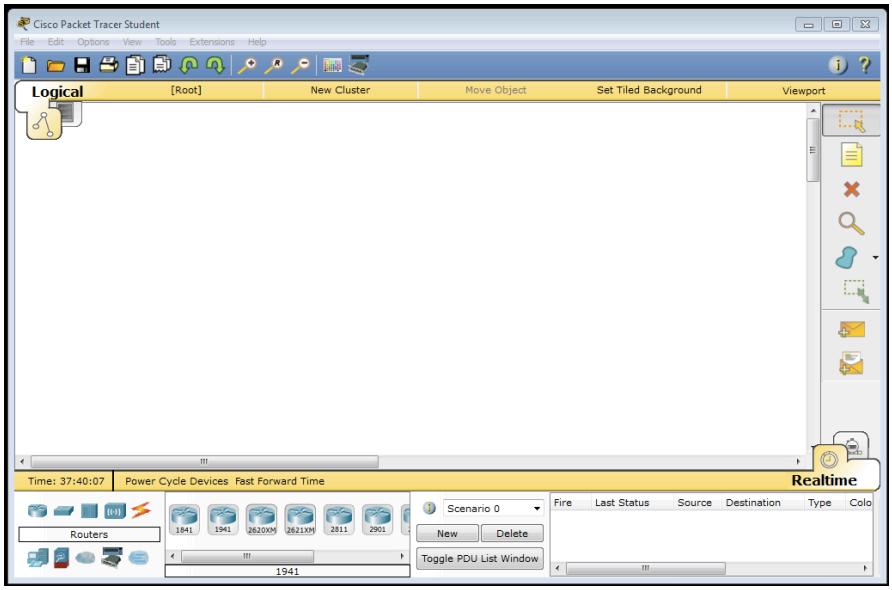

Figura 1: Ventana de inicio de Packet Tracer

Dispositivos

Para la creación de una red se pueden usar los dispositivos disponibles en la parte baja a la izquierda de la aplicación. Allí se puede escoger un disposivito de red entre routers, switches, hubs, dispositivo wireless o conexión.

Una vez elegido el tipo de dispositivo justo a la derecha se encuentran los que se pueden usar. Si por ejemplo se ha elegido routers, aquí aparecerán los diferentes modelos disponibles

Siempre abajo a la izquierda se pueden otros elementos útiles para las actividades prácticas como son los hosts (opción end devices).

Ejemplo de funcionamiento

Este programa tiene las normales funcionalidades que tiene todo programa como crear, abrir, guardar, ayuda, copiar, pegar, configuración de preferencias, etc. Esta funcionalidad no hace falta comentarlas aquí.

Para crear una red se puede elegir un dispositivo de los disponibles y simplemente arrastrarlo en la ventana principal. Supongamos por ejemplo que queremos crear la red de la Figura 2 que consiste de 6 PCs (hosts) distribuidos en tres redes.

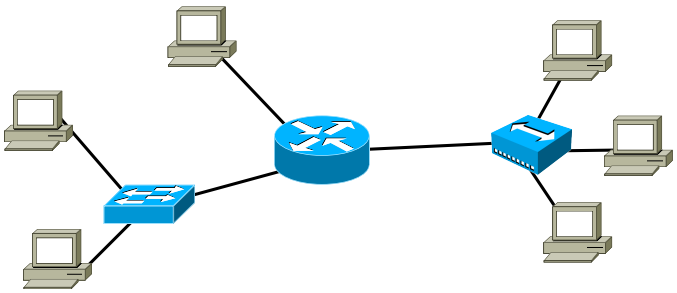

Figura 2: Red que se quiere configurar en Packet Tracer

Para crear esta red, simplemente se escogen 6 hosts (end devices) y se arrastran en la ventana principal.

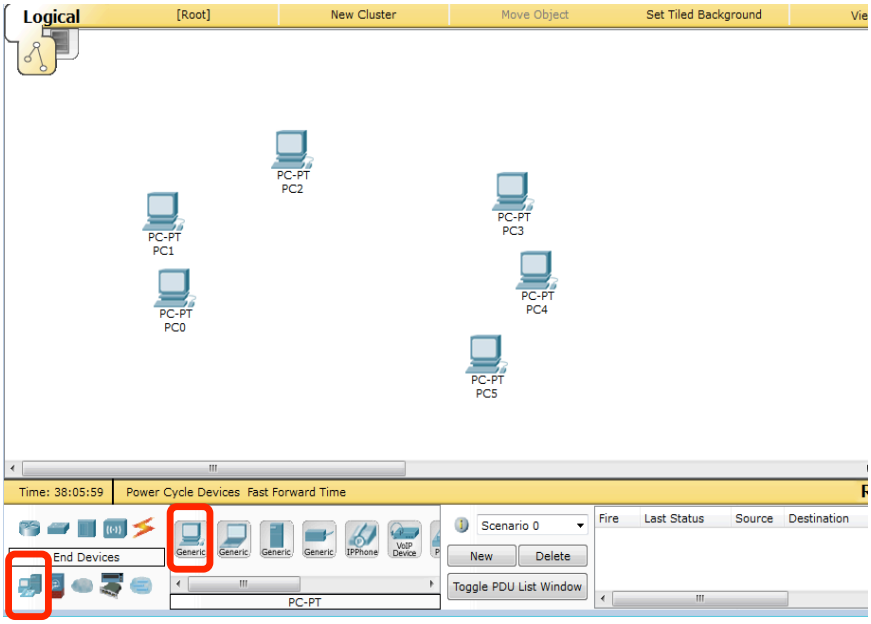

Figura 3: Se posicionan los PCs en Packet Tracer

De la misma forma, se escoge

- un hub (generic) que se usará para conectar PC3, PC4 y PC5 y el router,
- un switch (modelo 2950-24) que se usará para conectar PC0, PC1 y el router,
- un router (modelo 1841) que se usará para interconectar las redes.

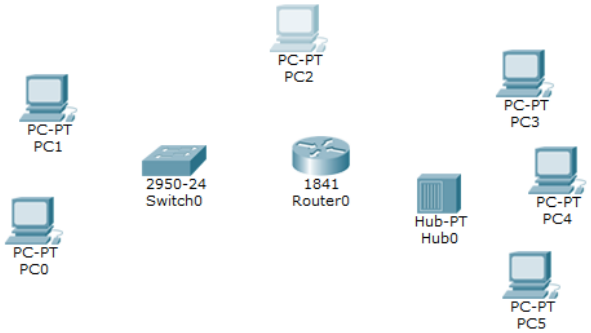

Figura 4: Se posicionan los demás dispositivos

Finalmente hay que interconectar entre sí los varios dispositivos. Conectamos PC0 y PC1 con el switch usando el elemento conexión (rayo rojo/amarillo) y escogemos la primera opción (automatically choose connection type).

Se hace lo mismo con el hub y PC3, PC4 y PC5.
De esta forma el sistema debería quedar de esta forma.

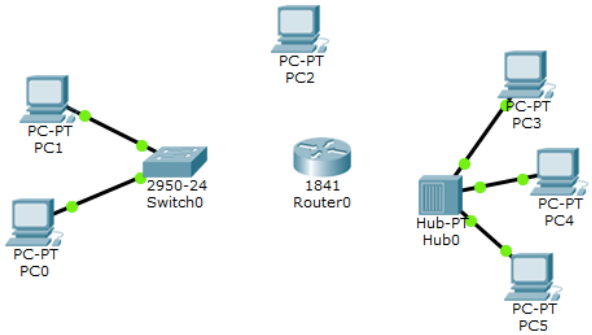

Figura 5: Se Conectan dos de las redes.

El último paso es conectar entre sí las redes usando el router.
Este router pero tiene a disposición solamente dos interfaces. Efectivamente, posicionando el cursor encima del router, aparece una ventana que nos informa del estado del router (Figura 6). En concreto informa que el router tiene dos interfaces del tipo fastethernet que etiqueta como FastEthernet0/0 y FastEthernet0/1. En esta ventana aparece también la etiqueta Vlan1; esta no es una interfaz real, se verá realmente que es más adelanta en una actividad práctica.

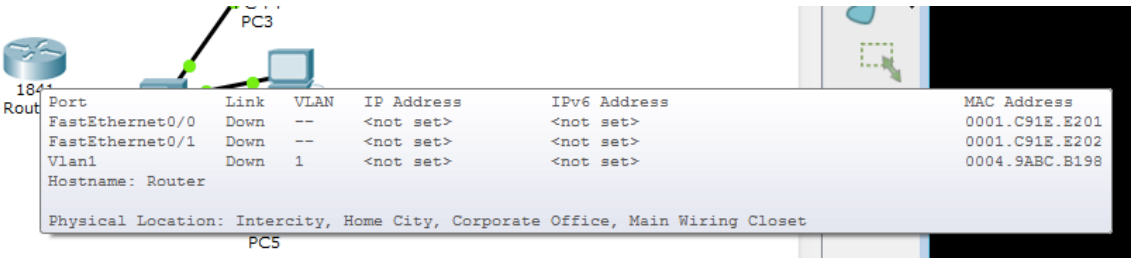

Figura 6: Estado del router.

Como el router tiene 2 interfaces, pero se necesitan 3, hay que instalar una interfaz nueva al router. Para hacer eso, hay que clicar encima del router para que se abra una nueva ventana (Figura 7).

Figura 7: Configuración del router.

En esta ventana hay tres pestañas:

- Physical enseña el aspecto que tiene la parte trasera del router (Physical Device View) y los modulos que se pueden instalar en este router.
- Config muestra la configuración actual del router y permite la configuración de algunos parámetros gráficamente.
- CLI (Command Line Interface) es la interfaz que permite operar con el Sistema Operativo del router (se verán más detalles en la primera actividad práctica).

En este ejemplo se quiere instalar una nueva interfaz al router. La primera operación es apagar el router. Luego se escoge un modulo que tenga una interfaz Ethernet y se arrastra a una de las dos ranuras disponibles (Figura 8).

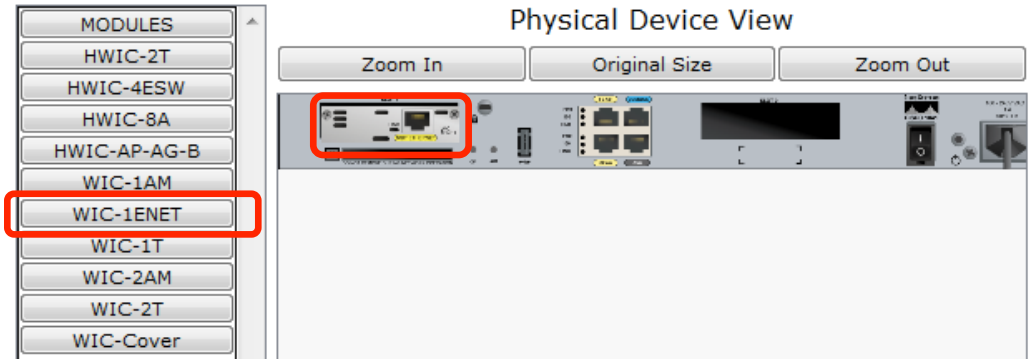

Figura 8: Se instala una nueva interfaz Ethernet en el router (mientras este está apagado).

Ahora el router tiene las tres interfaces necesarias y se pueden interconectar las tres redes del ejemplo usando conexiones (Figura 9).
Acordarse de volver a encender el router.

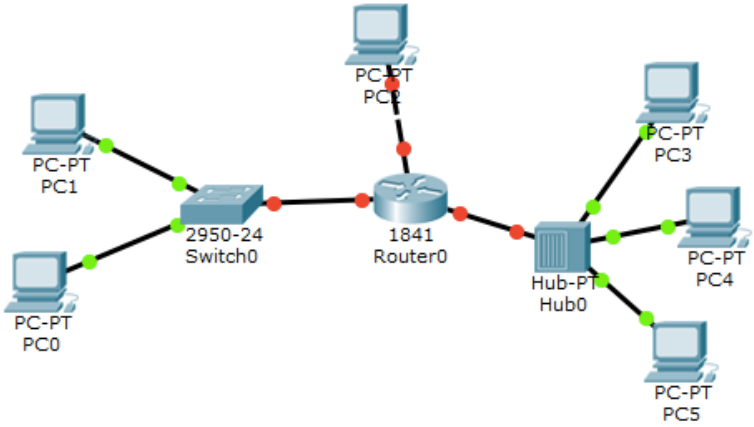

Figura 9: Resultado final.

Notar que algunas interfaces están indicadas en verde y otras en rojo. En concreto las rojas son aquellas conectadas al router. Esto porque las interfaces de los routers están desactivadas por defecto. Se verá en la primera actividad práctica como se configura y activa un router y sus interfaces, los switches y los PCs.

Lab. 1 – Configuración de IP y encaminamiento estático

1.1. Objetivo de la práctica

El objetivo de esta práctica es conocer los conceptos básicos de la configuración de direcciones IP (@IP) y tablas de encaminamiento en hosts y routers.

1.2. Configuración de hosts

1.2.1. Linux

1.2.1.1. Configuración de @IP

El comando que permite configurar interfaces de red en Linux es **ifconfig**. El formato de este comando es el siguiente

```
ifconfig interface @IPv4 netmask mascara broadcast @IPbroadcast
```

En negrita se indican los comandos necesarios y en itálico los que dependen de la configuración. Este comando activa la interfaz llamada *interface* y le asigna una @IPv4/mascara. Si no se asigna una mascara, esta dependerá de la clase de la @IP.

Por ejemplo, si se quiere configurar la @IP 10.0.0.10/24 a la interfaz eth1, el comando es

```
ifconfig eth1 10.0.0.10 netmask 255.255.255.0 broadcast 10.0.0.255
```

Los nombres de las interfaces los asigna el kernel automáticamente. Para visualizar las interfaces disponibles y su configuración actual, hay que ejecutar el comando

```
ifconfig -a
```

Tambien se puede activar o desactivar una interfaz con el comando

```
ifconfig eth1 up|down
```

El símbolo | indica parámetros alterbativos, es decir o bien se usa **up** para activa la interfaz o bien **down** para desactivarla

1.2.1.2. Configuración de rutas estaticas

El comando que permite añadir entradas manualmente en la tabla de encaminamiento es **route**. El formato de este comando es el siguiente

```
route add|del -net|-host destination [netmask mascara] gw @IPgateway
```

Tipicamente hay tres maneras para añadir una entrada en la tabla:

- el destino es un host concreto con su @IP, por ejemplo, el host 10.0.1.120 y se usa 10.0.0.1 como gateway

  ```
  route add -host 10.0.1.120 gw 10.0.0.1
  ```

- el destino es todos los dispositivos de una red concreta, por ejemplo, la red 10.0.2.0/24 y se usa 10.0.0.1 como gateway

  ```
  route add -net 10.0.2.0 netmask 255.255.255.0 gw 10.0.0.1
  ```

- el destino es todo el mundo (ruta por defecto), por ejemplo, usando 10.0.0.1 como gateway

  ```
  route add default gw 10.0.0.1
  ```

Para visualizar una tabla de encaminamiento se usa el comando

```
route -n
```

Lo que sale a continuación es la tabla de encaminamiento con indicado los destinos alcanzables por este host, el eventual gateway, la mascara y por que interfaz hay que enviar. Generalmente salen más parámetros, pero no son parte del objetivo de esta práctica.

```
route -n
Kernel IP routing table
Destination        Gateway        Genmask          Flags    Metric     Ref      Use       Iface
10.0.0.0           0.0.0.0        255.255.255.0    U        0          0        0         eth1
10.0.1.120         10.0.0.1       255.255.255.255  U        0          0        0         eth1
10.0.2.0           10.0.0.1       255.255.255.0    U        0          0        0         eth1
0.0.0.0            10.0.0.1       0.0.0.0          UG       0          0        0         eth1
```

1.2.2. Windows

En Windows hay varios programas que permite asignar @IP. Se recomienda el uso de **netsh** que se puede usar en la mayoría de versiones de Windows. Con netsh se puede o bien entrar en modo configuración simplemente arrancarndo la aplicación o configurar en la misma línea del comando.

En el primer caso, ejecutando netsh se visualiza este resultado

```
C:\Users\xyz\netsh
netsh>
```

Y se espera que se introduzcan los parámetros de configuración uno a uno a continuación.

O se puede directamente configurar añadiendo los parámetros después de netsh.

```
netsh interface ip set address name="NombreConexión" static @IP mascara [gateway] [metric]
```

En este caso, Windows da la posibilidad directa de asignar una ruta por defecto pasando por gateway.

Por ejemplo, si se quiere configurar la @IP 10.0.0.10/24 con gatewat 10.0.01, el comando es

```
netsh interface ip set address name="Local Area Connection" static 10.0.0.10 255.255.255.0 10.0.0.1
```

Los nombres de las interfaces los asigna Windows automáticamente. Para visualizar las interfaces disponibles y su configuración actual, hay que ejecutar el comando

```
netsh interface ip show config
```

Para visualizar la tabla de encaminamiento se usa el comando

```
netstat -r
```

Lo que sale a continuación es la tabla de encaminamiento con indicado los destinos alcanzables por este host, el eventual gateway, la mascara y por que interfaz hay que enviar. Generalmente salen más parámetros, pero no son parte del objetivo de esta práctica. A diferencia de Linux, en este caso no aparece la red propia y en la columna interfaz sale la @IP y no el nombre.

```
netstat -r
Network Destination     Netmask           Gateway       Interface     Metric
         10.0.1.120     255.255.255.255   10.0.0.1      10.0.0.10       266
         10.0.2.0       255.255.255.0     10.0.0.1      10.0.0.10       266
         0.0.0.0        0.0.0.0           10.0.0.1      10.0.0.10        10
```

1.2.3. Packet Tracer

Packet Tracer es un simulador que permite un limitado número de operaciones reales. En el caso de los hosts, por ejemplo, la configuración de una @IP y una ruta se hace directamente con una herramienta grafica. Se mantiene pero la posibilidad de visualizar el estado de las interfaces a través del command prompt.

El primer paso entonces es abrir la ventana de configuración de un host clicando encima de él. Esta ventana tiene 4 pestañas: Physical, Config, Desktop y Software/Services. Hay diferentes maneras para configurar un host. Lo que interesa para esta practica es la pestaña Desktop.

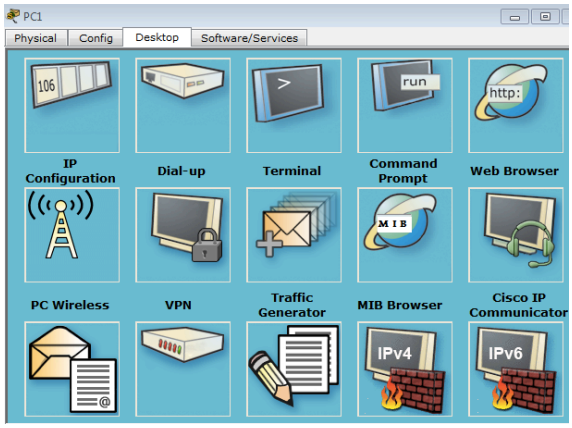

Figura 10: Pestaña Desktop de un host en Packet Tracer.

De las diferentes opciones interesan IP Configuration y Command Prompt. En IP Configuration se configura la @IP de host, su mascara y su ruta por defecto como se ilustra en el ejemplo de la Figura 11.

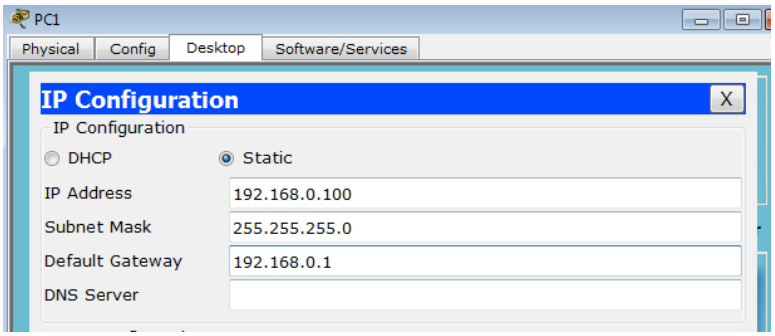

Figura 11: Ejemplo de configuración de un host en Packet Tracer.

La otra opción que interesa es el Command Prompt. La ventana que se abre permite interactuar con el host con comandos parecidos al Windows. De manera que se puede visualizar la @IP del host con ipconfig o la tabla de encaminamiento con netstat.

Tambien, pero es útil porque se pueden ejecutar algunas aplicaciones de interés como el ping o el tracert (traceroute en Linux) para verificar que la configuración del sistema es correcto como en el ejemplo de la Figura 11.

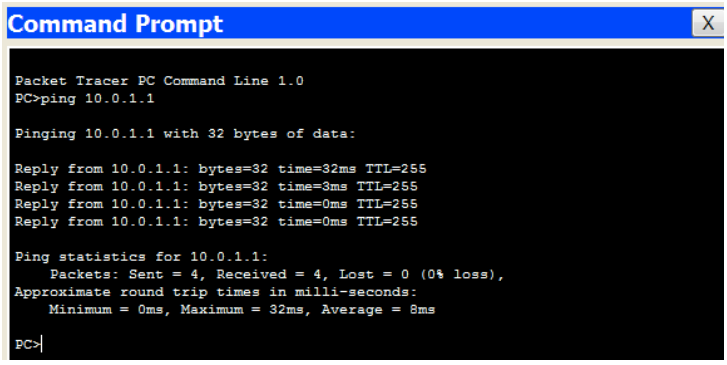

Figura 12: Uso del ping para verificar la conectividad entre dos @IP.

1.3. Configuración de routers

1.3.1. Estructura de un router

Un router IP es un ordenador especializado en encaminar datagramas IP. Dependiendo de las prestaciones que deba ofrecer, su estructura interna es más o menos compleja y especializada, pero para los modelos de gama baja, podemos pensar en una estructura similar a la de un PC: CPU, memoria, buses e interfaces de red. Para el almacenamiento de datos es habitual utilizar memoria ROM, memoria flash y memoria RAM y RAM no volátil (NVRAM):

- ROM: parte del sistema operativo y código de boot;
- Flash: imagen completa del sistema operativo;
- NVRAM: fichero de configuración por defecto del router;
- RAM: configuración actual del router.

Los sistemas operativos de los routers comerciales están especialmente diseñados para facilitar las tareas de conmutación de paquetes, la ejecución de algoritmos de encaminamiento, configuración de interfaces, etc. Un ejemplo de este tipo de sistemas operativos es el IOS (Internetworking Operative System) de CISCO. El IOS tiene una arquitectura simple y normalmente ocupa un espacio de memoria reducido. Cuando encendemos un router, se ejectua un programa de bootstrap cargado en la ROM que testea el sistema y carga en la RAM una imagen del IOS, normalmente desde la memoria flash.

El router se configura generalmente utilizando una interfaz de comandos en línea (CLI). Normalmente se hace a través de una conexión por la línea serie conectada al puerto CONSOLE del router, usando por ejemplo la aplicación HyperTerminal en Windows, MiniCOM en Linux, etc. Los parámetros necesarios para conectarse son los siguientes: Baud Rate 9600 bps, 8 bits/carácter, 1 bits de Stop, No paridad y No control de flujo Hardware. La configuración activa del router se encuentra en un fichero llamado running-config. Si apagamos el router, dicha configuración se perdería y no estaría presente al re-activar el router. Podemos guardar dicha configuración en un archivo de configuración (startup-config) que normalmente se graba en una memoria NVRAM. Al arrancar el router, la configuración que se activa es la guardada en el archivo startup-config.

También podemos configurar el router accediendo por telnet o utilizar un interfaz web para configurar el router. En estas prácticas se usará CLI.

1.3.2. Modos de configuración

Los router con IOS disponen de un conjunto de modos llamados de configuración que permiten la visualización y configuración del router. Los modos de configuración son los siguientes:

- Modo **BOOT** o **ROM monitor**: se usa en casos de emergencias (prompt típicamente rmon) como puede ser la recuperación de un password, de un registro de configuración, etc
- Modo de **SETUP**: permite una configuración por menu sencilla y básica del router
- Modo **USER EXEC**: es el modo de visualización sin privilegios (prompt R>)
- Modo **PRIVILEGED EXEC**: modo de visualización con privilegios (prompt R#)
- Modo de **Configuración Global** o **CONFIGURE**: permite configurar aspectos sencillos del router como pueden ser la configuración del nombre del router, passwords, etc (prompt R(config)#)
- Modo de **configuración específicos**: permiten configurar protocolos, interfaces o en general aspectos más complejos del router (prompt R(config-if)#, R(config-route)#, R(configline)#, etc).

Al arrancar el router podemos pasar al modo **SETUP**, que permite dar una primera configuración al router cuando éste carece de una configuración preestablecida, o bien pasar al modo **USER EXEC**, cuando el router sí dispone de una configuración preestablecida. El primer mensaje que emitirá el router es:

```
Continue with the configuration dialog [yes/no]:
```

A lo que habrá que contestar **NO** ya que se quiere configurar en línea a partir de USER EXEC.

En modo USER EXEC podemos consultar aspectos básicos de la configuración del router[1]. Para consultar aspectos más críticos de la configuración del router debemos pasar a modo PRIVILEGED EXEC. Entre USER EXEC y PRIVILEGED EXEC se puede configurar una contraseña de manera que solo los administradores pueden pasar a modos con más provilegios y de configuración.

Desde los modos USER EXEC y PRIVILEGED EXEC no se puede modificar la configuración del router. Para hacerlo se debe pasar del modo PRIVILEGED EXEC al modo de configuracion general (CONFIGURE). Desde allí se pueden configurar aspectos generales del funcionamiento del router o pasar a modos de configuración específicos de cada interfaz, algoritmo de encaminamiento, etc.

En la Figura 13 se muestran los diferentes modos de configuración junto con los principales commandos necesarios para cambiar de un modo a otro.

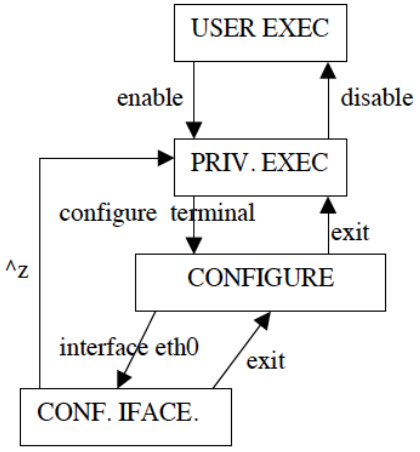

Figura 13: Modos de configuración de un router CISCO.

Por ejemplo

```
Router> <Comandos en modo USER EXEC>
Router> enable
Router# <Comandos en modo PRIVILEGED EXEC>
Router# configure terminal
Router(config)# <Comandos en modo CONFIGURE>
Router(config)# interface FastEthernet0/0
Router(config-if)# <Comandos en modo configuración especifica de la interfaz FastEthernet0/0>
Router(config-if)# exit
Router(config)# exit
Router# disable
Router>
```

1.3.3. Consulta de estado

Se puede consultar el estado de un router mediante el comando show. Dependiendo del tipo de información que se quiere consular, el comando se puede ejecutar en USER EXEC (no todo se puede ver) o en PRIV. EXEC si se quiere acceder a todo. Por ejemplo

- **show ip interface brief** muestra el estado de los interfaces, sus nombres y su configuración.
- **show running-config** muestra el fichero de configuración que está activo en el router
- **show startup-config** muestra el fichero de configuración que está grabado en la NVRAM
- **show ip <parameter>** muestra los parámetros asociado a la configuración del protocolo IP. Por ejemplo, la tabla de encaminamiento IP se consulta con **show ip route**
- **show interfaces** muestra la configuración de las interfaces

[1] Con el comando ? se puede obtener un listado de los comandos que se pueden ejecutar en cada modo.

La tabla de encaminamiento es una información que no se considera privilegiada y que puede ser consultada desde el modo usuario USER EXEC. Sin embargo, el contenido de los ficheros de configuración si que se consideran privilegiados y sólo pueden ser visualizados desde el modo PRIVILEGED EXEC.

1.3.4. Configuración de interfaces

Desde el modo de configuración se puede pasar a configurar las interfaces. Por ejemplo, para configurar una interfaz llamada Ethernet0 podemos hacer

```
Router# configure terminal
Router(config)# interface Ethernet0
Router(config-if)# ip address @IP mascara
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

Por ejemplo, para asignar la @IP 10.0.0.10/24 el comando es

```
Router(config-if)# ip address 10.0.0.10 255.255.255.0
```

Los nombres de las interfaces los asigna el IOS automáticamente. Para visualizar las interfaces disponibles, hay que ejecutar el comando

```
show ip interface brief
```

El comando **no shutdown** es necesario para activar la interfaz. Por defecto, todas las interfaces del router están desactivadas. Por el contrario, el comando **shutdown** desactiva la interfaz[2].

1.3.5. Encaminamiento estático

Para configurar encaminamiento estático hay que estar en modo CONFIGURE y aquí usar el commando **ip route**.

```
Router(config)# ip route @IP mascara @IPgateway
```

Por ejemplo, para añadir una ruta a la red 10.0.1.0/24 usando el gateway 10.0.0.1, el comando es

```
Router(config)# ip route 10.0.1.0 255.255.255.0 10.0.0.1
```

1.3.6. Verificación

Como se ha dicho anteriormente, se puede usar el comando show para verificar la configuración del router.

```
Router# show interfaces        Permite ver la configuración de las interfaces
Router# show ip route          Permite ver la tabla de encaminamiento
Router# show running-config    Permite ver la configuración actual del router
```

Pero también se puede usar la aplicación ping para verificar que hay conectividad con una determinada @IP. En este caso hay que ejecutar el ping desde modo visualización (USER o PRIV. EXEC).

1.3.7. Routers en Packet Tracer

En Packet Tracer hay disponibilidad de varios modelos de router de entre gama baja y media. Se recomienda usar para estas prácticas el modelo 1841 ya que tiene todas las funcionalidades necesarias y es idéntico al router real como se ve en la Figura 14.

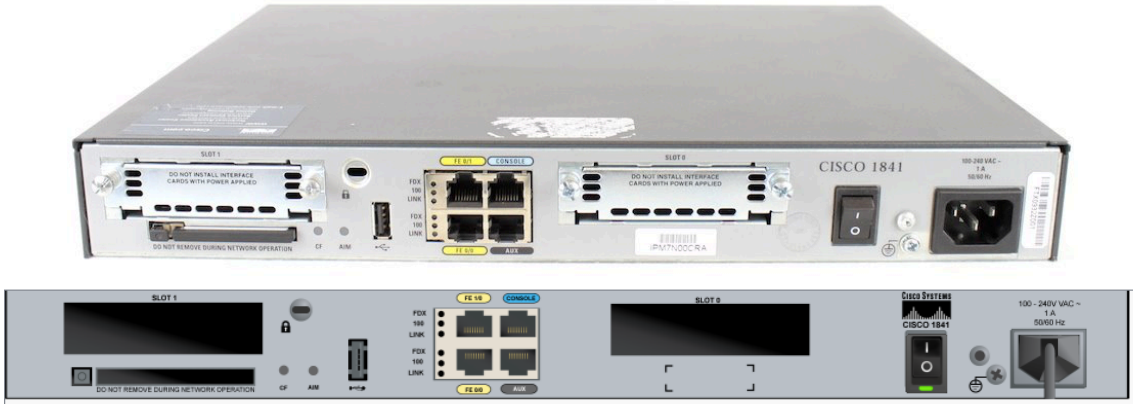

Figura 14: Router 1841 real y en Packet Tracer.

[2] La operación de anteponer un **no** delante de un comando es muy común en IOS y sirve para hacer la operación contraria. Así que si shutdown desactiva la interfaz, no shutdown la activa.

1.4. Realización de la práctica

1.4.1. Primera parte

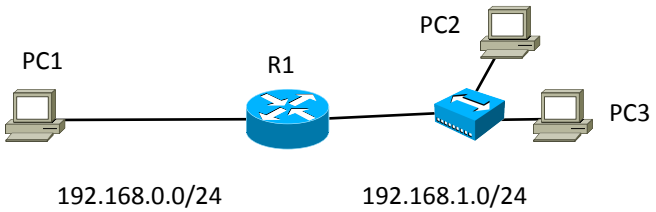

Figura 15: Configuración de la primera parte.

La Figura 15 representa la red de esta primera parte. Notar que se quieren configurar dos redes y se han indicado exclusivamente las direcciones de red. Las direcciones IP más bajas suelen usarse para las interfaces de los routers (porque son más fáciles de recorder, como por ejemplo 192.168.0.1), y las más altas para interfaces de los hosts (como por ejemplo 192.168.0.100).

Los pasos a seguir son los siguientes:

1. Elegir los dispositivos en Packet Tracer y conectarlos como en la figura.
2. Añadir al router una interfaz Ethernet como se explica en el capitulo anterior de introducción al entorno (se usará en la segunda parte).
3. Configurar los PCs (@IP y rutas).
4. Entrar en el CLI del router y configurarlo. Vigilar sobre que es lo que hay que configurar en este router.
5. Verificar que hay conectividad entre un cualquier PC y el router.
6. Verificar que hay conectividad entre cualquier pareja de PC.
7. Ver e interpretar las tablas de encaminamiento del router y de los PC.

1.4.2. Segunda parte

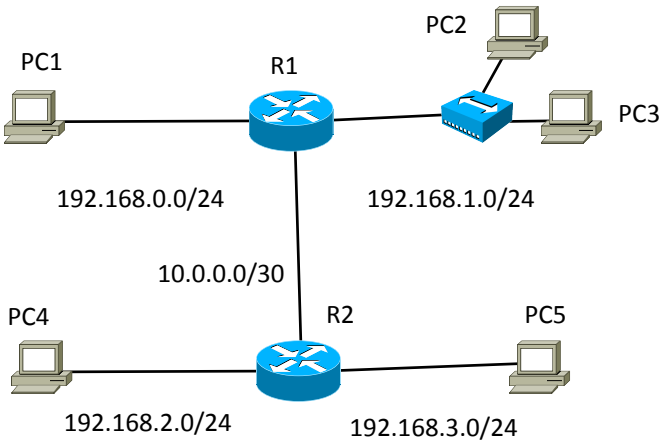

Figura 16: Configuración de la segunda parte.

La Figura 16 representa la red de esta segunda parte. Respecto al caso anterior se ha añadido un segundo router y dos PC más. Notar que también entre los dos router se forma una red.

Los pasos a seguir son los siguientes:

1. Añadir los dispositivos y conectarlos como en la figura.
2. Añadir al router una interfacz Ethernet.
3. Configurar los PCs (@IP y rutas).
4. Entrar en el CLI de los dos routers y configurarlos. Pensar bien como configurar las tablas de encaminamiento de los routers.
5. Verificar que hay conectividad entre un cualquier PC y el router y entre los dos routers.
6. Verificar que hay conectividad entre cualquier pareja de PC.

1.4.3. Entrega

Según el plazo marcado en el Campus Virtual, hay que entragar un informe usando la plantilla a disposición y respondiendo a las preguntas.

Lab. 2 – Encaminamiento dinámico con RIP

2.1 Objetivo de la práctica

El objetivo de esta práctica es familiarizarse con el concepto de encaminamiento dinámico y aprender a configurar routers con el protocolo RIP.

2.2 Routing Information Protocol

2.2.1 Introducción

Las características básicas son:

- Existen dos versiones, RIP version 1 (RIPv1, RFC 1058) y version 2 (RIPv2, RFC 2453).
- Usa un enfoque llamado vector-distancia.
- Los router envían periódicamente (cada 30 segundos) un mensaje RIP por cada interfaz con los destinos y métricas conocidos. Se envía con UDP, puerto origen y destino: 520. Los mensajes se envían a una dirección multicast que es la 224.0.0.9 (un datagrama con esta dirección destino llega a todos los routers RIP de la misma red que el origen).
- De toda la información que conoce (su tabla de encaminamiento), un router envía a un vecino solo aquella que no ha aprendido de la red común entre los dos (concepto de *split horizon*). Es decir, es inecesario enviar a un router información que se ha aprendido o bien de este o de otro router que comparte la misma red.
- Respecto a la versión 1, RIP versión 2 añade la máscara a los destinos enviados en los mensajes.
- La métrica es el número de redes que hay que cruzar para llegar destino: 1 si el destino es una red directamente conectada, 2 si hay que pasar por un router, etc.
    - Indica la "distancia" para llegar a una red.
    - La métrica maxima es 15.
    - La métrica infinito vale 16.
- Al recibir un mensaje RIP, un router compara el contenido con su tabla de encaminamiento y la modifica si
    - Descubre una nueva red.
    - Descubre una nueva ruta a una red ya conocida con una métrica extrictamente menor (si es igual no modifica).
    - La métrica de una ruta a una red ya conocida ha cambiado.
- Si se dejan de recibir mensajes RIP de un vecino durante 6 periodos (180 segundos), se asume que hay algún problema y se pone a 16 todas las métricas de las redes aprendidas de este vecino.

2.2.2 Configuración de RIP

Para activar el algoritmo de encaminamiento RIP, los pasos a seguir son los siguientes:

```
Router# configure terminal
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network @IPred1
Router(config-router)# network @IPred2
Router(config-router)# ...
Router(config-router)# exit
Router(config)#
```

El comando **network** indica las redes por donde enviar y por donde recibir mensajes de RIP. Se debe indicar las direcciones de red sin màscara.

Si se usa RIPv1, se asume una mascara correspondiente a la clase. Es decir, la red mayor a la que pertenece la dirección IP de la interfaz. Por ejemplo, si la interfaz usa la dirección IP 10.5.4.2, se anuncia la clase A de la forma **network 10.0.0.0**.

Si se quieren usar mascaras, hay que usar RIPv2. El uso de la versión 2 se indica después del comando **router rip**, ejecutando **version 2**.

```
Router(config)# router rip
Router(config-router)# version 2
```

2.2.3 Notas

Por defecto el router hace "sumarización de rutas". La sumarización se hace a la clase, y sólo cuando se envían los mensajes hacia una red con dirección base distinta. Por ejemplo, si en la tabla hay las redes 10.0.1.0/24 y 10.0.2.0/24, al enviar el mensaje RIP hacia la red 192.168.0.0/24 advertirá la red 10.0.0.0/8. Para desactivar la sumarización hay que ejecutar el comando:

```
Router(config)# router rip
Router(config-router)# no auto-summary
```

Para que el router advierta las entradas estáticas (esto incluye la entrada por defecto), hay que ejecutar el comando:

```
Router(config)# router rip
Router(config-router)# redistribute static
```

2.2.4 Verificación

Con el comando **show ip route** podemos observar la tabla de encaminamiento del router. En la información listada por el router, aparece indicado si la ruta se ha fijado de forma estática o ha sido aprendida con RIP.

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

 R  192.168.3.0/24 [120/1] via 192.168.0.2, 00:00:08, Serial0
```

En la entrada, la R indica que ha sido añadida por RIP. Un router usa dos métricas: la métrica administrativa y la métrica del algoritmo de encaminamiento. La métrica administrativa es el primer número entre corchetes e indica que protocolo de encaminamiento se está usando, siendo 120 el valor del RIP. El segundo número es la métrica usada por el protocolo RIP. La métrica de RIP mostrada por CISCO es el número de routers hasta el destino que es igual al número de redes menos 1. Es decir, en el caso que se muestra en el ejemplo, una métrica 1 en esta tabla significa que hay que cruzar 2 redes, si en la tabla estuviera un 2, entonces el número de redes sería 3, etc.

El comando **show ip protocol** permite ver la configuració de RIP. El comando muestra la versión de RIP tiene activada cada interfaz tanto de entrada (*receive*) como de salida (*sent*).

```
router# show ip protocol
 Routing Protocol is "rip"
   Sending updates every 30 seconds, next due in 8 seconds
   Invalid after 180 seconds, hold down 180, flushed after 240
   Outgoing update filter list for all interfaces is
   Incoming update filter list for all interfaces is
   Redistributing: rip
   Default version control: send version 2, receive version 2
   Interface       Send  Recv  Triggered RIP  Key-chain
   Ethernet2       2     2
   Ethernet3       2     2
```

En este ejemplo se muestra que los mensajes se envían cada 30 segundos y el siguiente se espera en 8 segundos. Se esperan 180 segundos sin recibir mensajes RIP antes de considerar un destino inalcanzable y pasados 60 segundos mas (240 en total), se elimina la entrada en la tabla de encaminamiento.

Finalmente se puede usar el comando **debug ip rip** (para desactivarlo es **no debug ip rip**). Con este comando, cada vez que se envía o recibe un mensaje RIP, se indica el contenido de este mensaje y por donde se ha enviado o se ha recibido. En el ejemplo a continuación se ve que se ha enviado un mensaje por la interfaz Ethernet0/1/0 (que tiene @IP 10.0.5.1) que contiene tres redes, la 10.0.0.0/24 y 10.0.1.0/24 ambas con métrica 2 y la 10.0.2.0/24 con métrica 1.

```
RIP: sending  v2 update to 224.0.0.9 via Ethernet0/1/0 (10.0.5.1)
RIP: build update entries
      10.0.0.0/24 via 0.0.0.0, metric 2, tag 0
      10.0.1.0/24 via 0.0.0.0, metric 2, tag 0
      10.0.2.0/24 via 0.0.0.0, metric 1, tag 0
```

En este otro ejemplo, se ve que se ha recibido un mensaje por la interfaz FastEthernet0/0 y se lo ha enviado un router con @IP 10.0.2.2. El mensaje contiene un único destino que es el 10.0.4.0/24 con métrica 1.

```
RIP: received v2 update from 10.0.2.2 on FastEthernet0/0
      10.0.4.0/24 via 0.0.0.0 in 1 hops
```

2.3 Ejemplo

Se quiere configurar RIP en los dos routers de la red de la Figura 17.

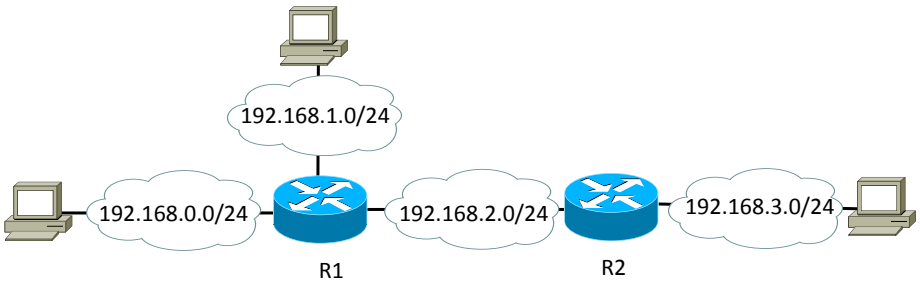

Figura 17: Ejemplo de red.

Solo se ilustran los comandos necesarios para el RIP, se supone que ya se han configurado @IP en las interfaces de los routers y también los hosts están ya configurados.

Al principio hay que activar todas las opciones necesarias para este ejemplo. Para los dos routers, hay que hacer

```
Router# configure terminal
Router(config)# ip routing              --> activa encaminamiento
Router(config)# router rip              --> activa RIP y se entra en configuración de RIP
Router(config-router)# version 2        --> se eligue la versión 2
Router(config-router)# no auto-sum      --> no se quieren agrupar redes
```

Luego hay que configurar de manera especifica cada router para que anuncie y reciba mensajes RIP. Para el router R1 es

```
Router(config)# router rip                    --> se entra en configuración de RIP
Router(config-router)# network 192.168.0.0
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
```

Como se puede observar hay que indicar todas aquellas redes conectadas directamente al router R1. De la misma forma, en el router R2 hay que activar el RIP en estas dos redes

```
Router(config)# router rip                    --> se entra en configuración de RIP
Router(config-router)# network 192.168.2.0
Router(config-router)# network 192.168.3.0
```

Fijarse que también se pone la red común entre los dos routers.

Estos comandos son suficientes para que las tablas de encaminamiento de los dos routers se completen correctamente. Por ejemplo, si se mirase la tabla de encaminamiento de R1 se vería

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

 C  192.168.0.0/24 is directly connected, FastEthernet0/0
 C  192.168.1.0/24 is directly connected, FastEthernet0/1
 C  192.168.2.0/24 is directly connected, Ethernet0/1/0
 R  192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:08, Ethernet0/1/0
```

Donde efectivamente la red 192.168.3.0/24 se ha aprendido con RIP y el gateway es el 192.168.2.2 que es la interfaz del router R2. Se ve que la métrica administrativa es 120 (indica que es RIP) y que la métrica es 1. Recordar que en CISCO este valor indica el número de routers que hay que cruzar para llegar a la red destino. Para conocer la métrica real RIP hay que sumarle 1 (número de redes que hay que cruzar).

2.4 Realización de la práctica

2.4.1 Primera parte

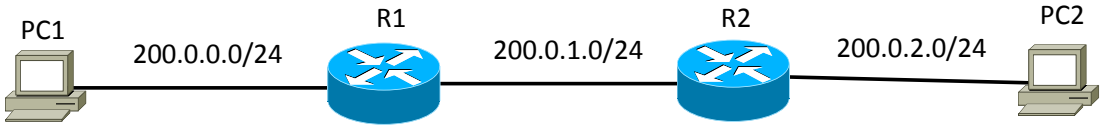

Figura 18: Configuración de la primera parte.

La Figura 18 representa la red de esta primera parte. Notar que se quieren configurar tres redes y se han indicado exclusivamente las direcciones de red.

Los pasos a seguir son los siguientes:

1. Elegir los dispositivos en Packet Tracer y conectarlos como en la figura.
2. Añadir a los dos routers una interfaz Ethernet como se explica en el capitulo de introducción al entorno (se usará en la segunda parte).
3. Configurar los PCs (@IP y rutas).
4. Entrar en el CLI de cada router y configurar las @IP.
5. Activar el RIPv2 como se ha explicado anteriormente en los dos routers.
6. Verificar que hay conectividad entre un cualquier PC y el router.
7. Verificar que hay conectividad entre cualquier pareja de PC. Verificar el camino entre PC1 y PC2 con tracert.
8. Ver e interpretar las tablas de encaminamiento del router y de los PC.
9. Activar el debug ip rip en un router e interpretar los mensajes.

2.4.2 Segunda parte

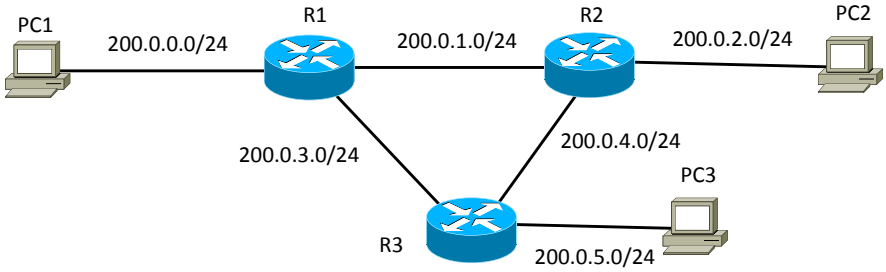

Figura 19: Configuración de la segunda parte.

La Figura 19 representa la red de la segunda parte. Notar que es continuación del anterior y hay que añadir 3 redes, un router y un PC.

Los pasos a seguir son los siguientes:

1. Añadir un router y un PC y conectarlos como en la figura.
2. Añadir al router una interfaz Ethernet.
3. Configurar el PCs (@IP y ruta por defecto).
4. Entrar en el CLI de los tres routers y configurar las @IP.
5. Modificar la configuración del RIPv2 en los routers R1 y R2 y activarlo en el router R3.
6. Verificar que hay conectividad entre todos los PC.
7. Verificar el contentido de la tabla de encaminamiento de los tres routers.
8. Activar el debug ip rip en el router R3 y probar a desconectar el cable que conecta R1 con R2.
9. Ver como actua RIPv2 en este caso (notar los mensajes con métrica 16) y verificar que sigue habiendo conectividad entre los PC. Verificar cual es ahora la ruta entre PC1 y PC2.

2.4.3 Entrega

Según el plazo marcado en el Campus Virtual, hay que entragar un informe usando la plantilla a disposición y respondiendo a las preguntas.

Lab. 3 – Configuración de VLAN

3.1 Objetivo de la práctica

El objetivo de esta práctiva es familizarizarse con el concepto de Virtual Local Area Network (VLAN) y aprender a configurar VLAN en switches y routers usando el protocolo IEEE802.1Q.

3.2 Switches

3.2.1 Introducción

Un switch Ethernet es un dispositivo de nivel 2 que segmenta los dominios de colisiones. La configuración de un switch es totalmente dependiente del fabricante. En esta práctica vamos a usar switches Ethernet de la gama 2950 de CISCO. Para entrar y configurar el switch seguiremos los mismos pasos que en un router CISCO. Clicando encima del swith, se abre una ventana donde salen 3 pestañas: Physical, Config y CLI. La primera muestra el aspecto físico del switch, la segunda permite ver la configuración del switch de manera visual y finalmente CLI permite conectarnos al switch y configurarlo a través de su sistema operativo. El sistema operativo es idéntico al del router con la diferencia que los comandos son algo distintos y propios de configuración de un switch.

Una vez conectados al CLI, se entra en modo user exec. De modo user exec, se entra a modo privilegiado con el comando **enable**. En este modo, se pueden visualizar tablas, ficheros de configuración (running-config), bases de datos del switch, etc. Para configurar cualquier funcionalidad hay que entrar en el modo de configuración global usando el comando **configure terminal**.

3.2.2 Tabla MAC

Cada puerto de un switch es un dominio de colisiones. Para segmentar la red Ethernet, un switch usa una table, llamada tabla MAC. El switch inicialmente tiene esta tabla vacía. Cada vez que una estación envía una trama Ethernet a otro host, el switch aprende a que interfaz está conectado una dirección MAC. Por ejemplo, si una trama Ethernet entra por la interfaz del switch fe0/0 con dirección MAC origen 00-11-22-33-44-55 y tiene MAC destino 00-66-77-88-99-AA, el switch aprende que la MAC 00-11-22-33-44-55 está conectada a la interfaz fe0/0.

A medida que los hosts envían tramas a otros hosts y estos responden, la tabla MAC del switch se va llenando. Como los hosts pueden cambiar de situación (pasar a estar conectados a otra interfaz), no conviene que las entradas de la tabla MAC sean estáticas. Por eso las entradas tienen un tiempo de vida llamado **age**. Pasado este tiempo de vida, la entrada de la tabla MAC desaparece (*aging out*). Por eso se dice que las entradas son dinámicas.

Por defecto un switch CISCO de gama 2950 tiene asignado un tiempo de vida por defecto en la tabla MAC de 300 segundos (5 minutos), mecanismo de aprendizaje dinámico y ninguna estrada estática en la tabla.

Para consultar y gestionar una tabla MAC de un switch se pueden usar estos commandos

```
Switch# show mac-address-table               --> Visualiza el contenido de la tabla MAC
Switch# show mac-address-table aging-time    --> Visualiza el tiempo de vida de las entradas de la
                                                  tabla MAC

Switch# clear mac-address-table dynamic      --> Elimina todas las entradas de la tabla MAC
Switch# clear mac-address-table dynamic interface INTERFAZ   --> Elimina la MAC asociada a la
                                                                  interfaz INTERFAZ de la tabla MAC
```

3.3 VLAN

3.3.1 Introducción

Se define una VLAN como una red IP. Cada una de las interfaces de un router es una red IP por definición. Para ahorrar interfaces de router se pueden crear redes IP en un switch mediante software. Eso significa que con una interfaz de router conectado al switch se pueden crear tantas VLANs (redes IP) como el software del switch permita. Un switch CISCO de la gama 2950 permite crear hasta 1024 VLANs.

Por lo tanto, si una interfaz de router debe soportar N VLANs (N redes IP) la interfaz deberá tener N direcciones IP, una por cada VLAN creada. Para ir de una VLAN a otra los datagramas deberán entonces obligatoriamente pasar por el router (que hará encaminamiento entre las dos VLANs); es decir, no se puede ir de una VLAN a otra directamente a través del switch. Del mismo modo, las tramas no se propagan entre VLANs distintas. Para conseguir esta segmentación de nivel 3 se utiliza un protocolo específico llamado de **trunking**. Este protocolo permite definer los enlances de dos modos diferentes. Por un lado, un enlace en modo **access** será de una VLAN especifica. Por otro lado, un enlance en modo **trunk** podrá pertencer a más de una VLAN, de modo que se permite enviar por este enlace todo el tráfico de VLANs diferentes (tipocamente del switch al router).

Un switch necesita una tabla para gestionar las tramas según su VLAN origen y VLAN destino. Esta tabla contiene por un lado las VLAN creadas y por el otro las interfaces asignadas a una determinada VLAN; estas asignaciones pueden ser

estáticas (no cambian en el tiempo) o dinámicas (pueden cambiar en el tiempo de manera automática según algún criterio). En esta asignatura, solo se trata el caso estático. Con esta información y con la tabla MAC, el switch es capaz de reconocer por donde enviar una trama, es decir si hacía una interfaz de una VLAN concreta (si la VLAN origen y destino coinciden) o hacía la interfaz de trunk (si las VLANs no coinciden).

Existen dos protocolos de trunking: el que se usó por primera vez, propietario de CISCO, conocido como ISL, y el estandarizado por el IEEE: IEEE802.1Q. En los equipos de CISCO se pueden encontrar ambos protocolos (los equipos más modernos suelen llevar sólo IEEE802.1Q). Los switches 2950 también disponen solamente de IEEE802.1Q.

3.3.2 Configuración de un switch

Cuando se enciende un switch CISCO, todas las interfaces pertenecen a la VLAN nativa. La VLAN nativa por definición es la VLAN identificada con el número 1. Si se define una VLAN para un uso específico es mejor usar otras VLAN-ID distintos al 1. Para definir VLANs en un switch hay que seguir estos pasos:

```
Switch# vlan database
Switch(vlan)# vlan VLAN-ID name NOMBRE
Switch# exit
```

donde VLAN-ID es un número entre 1 y 1005 (se recuerda que la 1 ya está creado por defecto) y NOMBRE es un nombre cualquiera que se quiere asignar a la VLAN creada. Cabe destacar que ademas de la VLAN 1, también las VLANs 1002, 1003, 1004 y 1005 ya están creadas por defecto y se pueden usar exclusivamente para tecnologías determinadas (FDDI, Token Ring, etc.) que no se comentan en esta asignatura.

Por ejemplo, para crear la VLAN 2 con nombre AXSI, el comando es

```
Switch(vlan)# vlan 2 name AXSI
```

Los comandos para visualizar información sobre las VLANs son

```
Switch# show vlan             --> visualiza las VLAN creadas y como están asignadas las interfaces
Switch# show vlan id VLAN-ID  --> visualiza los parámetros de la VLAN con número VLAN-ID
```

Una vez que la VLAN está creada hay que asignar interfaces a la VLAN. Usar el comando switchport para asignar de forma estática puertos a una VLAN

```
Switch# configure terminal
Switch(config)# interface FastEthernet0/0           --> se entra en la configuración de esta interfaz
Switch(config-if)# switchport mode access           --> se define como una interfaz de una VLAN
Switch(config-if)# switchport access vlan VLAN-ID   --> se asigna a la VLAN con número VLAN-ID
Switch(config-if)# exit
```

Aquella o aquellas interfaces que son de todas las VLAN, hay que configurarla en modo trunk. En este caso la interfaz tiene que estar asignada a la VLAN nativa (VLAN=1). Solo interfaces Fast Ethernet pueden ser trunk.

```
Switch# configure terminal
Switch(config)# interface FastEthernet0/10   --> se entra en la configuración de esta interfaz
Switch(config-if)# switchport mode trunk     --> se define como interfaz trunk
Switch(config-if)# exit
```

3.3.3 Configuración de un router

Tambien hay que configurar el router para que entienda las diferentes VLANs creadas. Los comandos siguientes son para los routers de la gama 1841. El enlace del router debe ser un enlace **trunk** y además debe tener tantas direcciones IP como VLANs creadas. Para ello crearemos subinterfaces en la interfaz FastEthernet del router (debe ser FastEthernet). A cada subinterfaz hay que asignarle una VLAN y darle una @IP.

En el siguiente ejemplo se supone que hay 2 VLANs (la VLAN 2 y VLAN 3) y se usa la interfaz FastEthernet0/0 como interfaz de partida para crear las dos subinterfaces FastEthernet0/0.1 y FastEthernet0/0.2. A cada subinterfaz hay que asignar una VLAN y una @IP.

```
Router# configure terminal
Router(config)# interface FastEthernet0/0    --> se entra en la configuración de esta interfaz
Router(config-if)# no ip address             --> no se asigna una @IP a la interfaz
Router(config-if)# interface FastEthernet0/0.1  --> se crea la primera subinterfaz
Router(config-subif)# encapsulation dot1q 2     --> se asigna la VLAN 2
Router(config-subif)# ip address @IP MASCARA    --> se asigna una @IP y una mascara
Router(config-subif)# exit
Router(config-if)# interface FastEthernet0/0.2     --> se crea la segunda subinterfaz
Router(config-subif)# encapsulation dot1q 3     --> se asigna la VLAN 3
Router(config-subif)# ip address @IP MASCARA    --> se asigna una @IP y una mascara
Router(config-subif)# exit
```

Notar que en la tabla de encaminamiento tiene que aparecer una entrada con cada subinterfaz y su red IP.

3.3.4 Verificación

```
Switch# show vlan               --> visualiza las VLAN creadas y como están asignadas las interfaces
Switch# show vlan id VLAN-ID    --> visualiza los parámetros de la VLAN con número VLAN-ID
Switch# show interfaces         --> visualiza el estado de todas las interfaces
```

```
Switch# show running-config      --> visualiza la configuración del switch
Switch# show mac-address-table   --> visualiza el contenido de la tabla MAC

Router# show ip route
Router# show running-config
```

3.4 Ejemplo

En este ejemplo, hay que configurar 2 VLAN identificadas como 2 y 3 con direcciones de red 10.0.0.0/24 y 10.0.1.0/24 respectivamente.

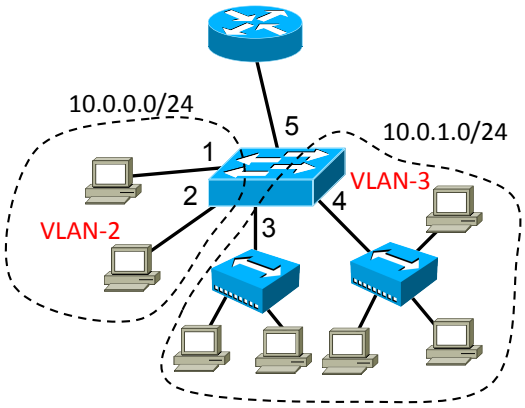

Figura 20: Ejemplo.

Solo se ilustran los comandos necesarios para la configuración de las VLAN, se supone que ya se han configurado los hosts.

Al principio hay que configurar el switch creando las dos VLAN que se llamarán RED1 y RED2.

```
Switch# vlan database
Switch(vlan)# vlan 2 name RED1
Switch(vlan)# vlan 3 name RED2
Switch(vlan)# exit
```

Luego se configuran las interfaces supiniendo que todas se llaman FastEthernet0/ seguido de el número de la interfaz.

Se configuran las dos interfaces de la VLAN-2 de esta forma.

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
```

Se configuran las dos interfaces de la VLAN-3 de esta forma.

```
Switch(config)# interface FastEthernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config-if)# exit
Switch(config)# interface FastEthernet0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config-if)# exit
```

Y finalmente la interfaz 5 que es la de trunk.

```
Switch(config)# interface FastEthernet0/5
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

Luego se configura el router creando dos subinterfaces y asignando a cada una una @IP propia de la VLAN.

```
Router(config)# interface FastEthernet0/0
Router(config-if)# no ip address
Router(config-if)# no shutdown
Router(config-if)# interface FastEthernet0/0.1
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# ip address 10.0.0.1 255.255.255.0
Router(config-subif)# exit
Router(config-if)# interface FastEthernet0/0.2
Router(config-subif)# encapsulation dot1q 3
Router(config-subif)# ip address 10.0.1.1 255.255.255.0
Router(config-subif)# exit
```

3.5 Realización de la práctica

3.5.1 Primera parte

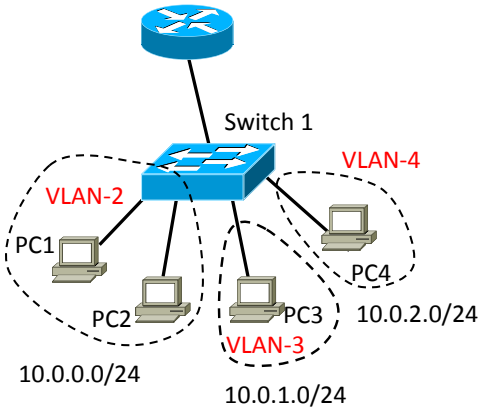

Figura 21: Configuración de la primera parte.

La Figura 21 representa la red de esta primera parte. Notar que se quieren configurar tres VLAN y se han indicado exclusivamente las direcciones de red.

Los pasos a seguir son los siguientes:

1. Elegir los dispositivos en Packet Tracer y conectarlos como en la figura. Elegir el Switch modelo 2950-24.
2. Configurar los PCs (@IP y rutas).
3. Entrar en el CLI del switch, crear las tres VLAN y asignar las interfaces del switch a las VLAN.
4. Configurar la interfaz de trunk.
5. Entrar en el CLI del router y configurar las @IP a las subinterfaces. Acordarse de activar la interfaz.
6. Verificar que hay conectividad entre cualquier pareja de PC.
7. Verificar cual es el camino (usar tracert) entre PC de una misma VLAN y entre PC en VLAN diferentes.
8. Ver e interpretar las tablas de encaminamiento del router y de los PC.

3.5.2 Segunda parte

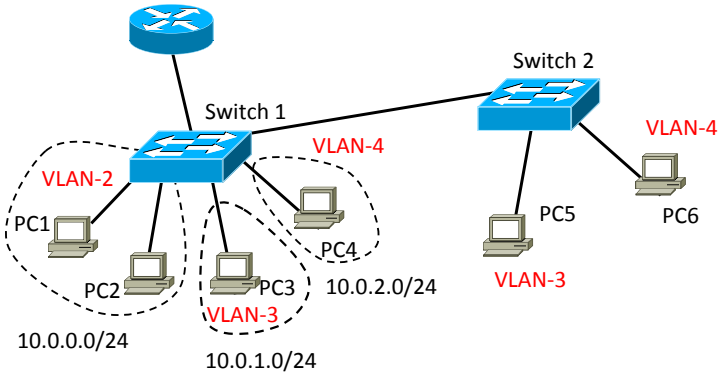

Figura 22: Configuración de la segunda parte.

La Figura 22 es la red de la segunda parte. Notar que es continuación del anterior y hay que añadir un switch y dos PC.

Los pasos a seguir son los siguientes:

1. Añadir un switch y dos PC y conectarlos como en la figura.
2. Configurar el PCs (@IP y ruta por defecto).
3. Entrar en el CLI del Switch2, crear las VLAN 3 y 4 y asignar las interfaces a las VLAN.
4. Configurar la interfaz de trunk. ¿Hace falta hacer algo en el Switch1? Pensarlo bien.
5. Verificar que hay conectividad entre todos los PC.
6. Verificar el camino para ir de PC5 a PC3, de PC5 a PC6 y de PC1 a PC6.

3.5.3 Entrega

Según el plazo marcado, entragar un informe con nombre y apellido y rellenando la plantilla de esta practica 3 disponible en la sección de entregas de la Intranet.

Lab. 4 – Configuración de NAT

4.1 Objetivo de la práctica

El objetivo de esta práctiva es familizarizarse con el mecanismo NAT y saber configurar un router con tres diferentes tipos de NAT.

4.2 Network Address Translation

4.2.1 Introducción

NAT es el proceso que permite la tradución de direcciones privadas a públicas mediante la substitución o alteración de las direcciones IP o puertos en las cabeceras IP y TCP del paquete transmitido. Para que NAT funcione se debe disponer de un router que implemente NAT en alguna o varias de sus variantes: NAT estático, NAT dinámico y NAT por puertos (PAT).

Aunque en esta práctica se usará para esta function, NAT no se usa exclusivamente para traducir direcciones privadas a públicas. Hay ocasiones en que se traducen direcciones privadas a privadas o direcciones públicas a direcciones públicas. Por consiguiente, se usa la siguiente nomenclatura genérica a la hora de usar NAT:

- **Direcciones Internas** (Inside addresses): aquella que se quieren traducir
- **Direcciones Externas** (Outside addresses): aquella a la que se traduce

Las direcciones internas pueden ser tanto privadas como públicas. El caso más típico es aquel en que la dirección interna es una dirección privada y la dirección externa es una dirección pública. La clasificación anterior se puede subdividir a su vez:

- **Direcciones locales internas** (Inside local addresses): la dirección IP interna asignada a un host en la red interna
- **Direcciones globales internas** (Inside global addresses): la dirección IP de un host en la red interna tal como aparece a una red externa
- **Direcciones locales externas** (Outside local addresses): la dirección IP de un host externo tal como aparece a la red interna
- **Direcciones globales externas** (Outside global addresses): la dirección IP asignada a un host externo en una red externa

En resumen, la diferencia entre una dirección local interna y una global interna es que la primera es la dirección que se quiere traducir mientras que la segunda es la dirección ya traducida.

4.2.2 NAT estático

Se usa NAT estático cuando las direcciones están almacenadas en una tabla de consulta del router y se establece un mapeo directo entre las direcciones internas locales y las direcciones internas globales. Eso significa que por cada dirección interna local existe una dirección interna global. Este mecanismo se suele usar cuando se quiere cambiar un esquema de direcciones de una red a otro esquema de direcciones o cuando se tienen servidores que tienen que mantener una dirección IP fija de cara al exterior como DNS o servidores Web.

Para configurar NAT estático se siguen los siguientes pasos:

1) Definir el mapeo de las direcciones estáticas:

   ip nat inside source static *@IP-local @IP-global* → para configurar el NAT de 1 @IP

   ip nat inside source static network *red-local red-global mascara* → para configurar el NAT de toda una red

2) Especificar la interfaz interna

   ip nat inside

3) Especificar la interfaz externa

   ip nat outside

Considerando el ejemplo de la Figura 23, donde la dirección IP privada 10.1.1.1 es la interna y la @IP externa es la pública 201.3.1.4.

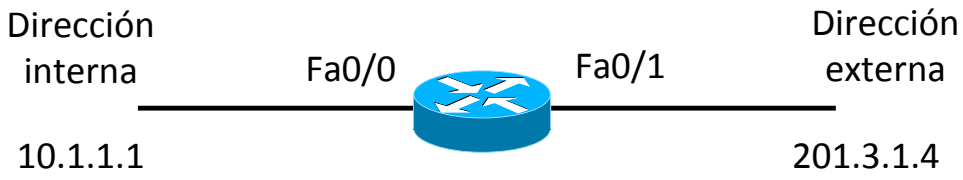

Figura 23: Ejemplo de NAT estático

En este caso la configuración correcta del router es la siguiente

```
Router# configure terminal
Router(config)# ip nat inside source static 10.1.1.1 201.3.1.4
Router(config)# interface Fa0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface Fa0/1
Router(config-if)# ip nat outside
Router(config-if)# exit
```

4.2.3 NAT dinámico

Se usa NAT dinámico cuando se dispone de un conjunto de direcciones globales internas que se asignarán de forma dinámica y temporal a las direcciones locales internas. Esta asignación se efectua cuando se recibe el primer datagrama en el router y tiene una duración limitada. Este mecanismo se suele usar cuando se quiere evitar que equipos externos empiezen una comunicación con equipos internos y para reducer el número de @IP publicas reservadas.

Para configurar NAT dinámico se siguen los siguientes pasos:

1) Crear un conjunto de direcciones globales:

   ip nat pool *nombre @IP-global-inicial @IP-global-final {***netmask** *mask}*

2) Crear una ACL que identifique a los hosts para la traslación

   access-list *numero* **permit** *@IP-red-interna wildcard*

   donde la wildcard se puede interpreter como el inverso de la mascara (se verá mejor en la práctica 5), es decir se substituyen lo 0 con los 1 y viceversa. Por ejemplo, la mascara 255.255.0.0 es la wildcard 0.0.255.255.

3) Configurar NAT dinámico basado en la dirección origen asociando el número de la access-list con el nombre del rango de direcciones globales

   ip nat inside source list *numero* **pool** *nombre*

4) Especificar la interfaz interna

   ip nat inside

5) Especificar la interfaz externa

   ip nat outside

Considerando el ejemplo de la Figura 24, donde el grupo de dirección IP privada 10.1.1.0/24 son internas y se ha reservado un rango de 30 direcciones externas 201.3.1.1-201.3.1.30 públicas.

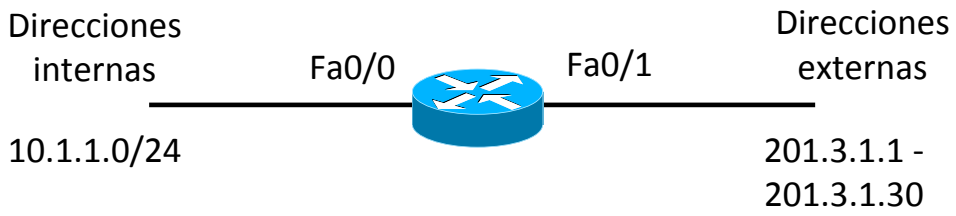

Figura 24: Ejemplo de NAT dinámico

En este caso la configuración correcta del router es la siguiente

```
Router# configure terminal
Router(config)# ip nat pool lab4 201.3.1.1 201.3.1.30 netmask 255.255.255.0
Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 pool lab4
Router(config)# interface Fa0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface Fa0/1
Router(config-if)# ip nat outside
Router(config-if)# exit
```

Las entradas se asignan por defecto 24 horas. Si se quiere modificar el valor del temporizador usar el siguiente comando:

```
Router(config)# ip nat translation timeout seconds
```

Donde *seconds* es la duración de una traducción dinámica del NAT.

4.2.4 PAT

Se usa PAT (NAT por puertos o NAT overload) cuando todo un conjunto (centenares) de direcciones locales internas se quieren traducir a una única dirección global interna. Esta asignación la efectúa el router modificando el par @IP/puerto. Aunque se disponga de 65535 puertos (16 bits) en realidad un router que implementa PAT solo puede usar un subconjunto

de estos puertos (depende del router, pero aproximadamente unos 4000 puertos por dirección global). Eventualmente, PAT se puede usar juntamente con NAT dinámico de forma que un mayor número de direcciones locales internas se pueden traducir a varias direcciones globales con múltiples puertos.

Para configurar PAT se siguen los siguientes pasos:

1) Crear un conjunto de direcciones globales

ip nat pool *nombre @IP-global-inicial @IP-global-final*

2) Crear una ACL que identifique a los hosts para la traslación

access-list *numero* **permit** *@IP-red-interna wildcard*

3) Configurar NAT dinámico basado en la dirección origen asociando el número de la access-list con el nombre del rango de direcciones globales

ip nat inside source list *numero* **pool** *nombre* **overload**

4) Especificar la interfaz interna

ip nat inside

5) Especificar la interfaz externa

ip nat outside

Considerando el ejemplo de la Figura 25, donde el grupo de dirección IP privada 10.1.1.0/24 son internas y pueden usar la dirección pública 201.3.1.10 del router.

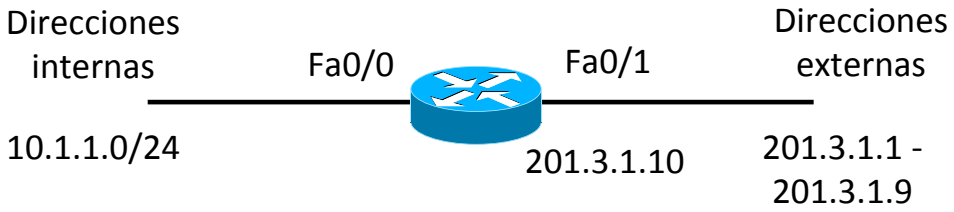

Figura 25: Ejemplo de PAT

En este caso la configuración correcta del router es la siguiente

```
Router# configure terminal
Router(config)# ip nat pool lab4 201.3.1.10 201.3.1.10 netmask 255.255.255.0
Router(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 pool lab4 overload
Router(config)# interface Fa0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface Fa0/1
Router(config-if)# ip nat outside
Router(config-if)# exit
```

Ya que solo hay una @IP publica que es la del router, se puede sustituir el primer y el tercer comando de la configuración del nat (la access-list 1 se sigue necesitando) con este único comando:

```
Router(config)# ip nat inside source list 1 interface Fa0/1 overload
```

En el caso de que haya un conjunto de direcciones globales, se puede usar PAT juntamente con NAT dinamico. En este caso simplemente se configura el rango (pool) de dirección como en el caso de NAT dinamico donde una de estas @IP se usa también para el router.

4.3 Verificación

```
Router# show ip nat translation            --> se consulta la tabla NAT
Router# show ip nat translation verbose    --> se consulta la tabla NAT con más informaciónn
Router# show ip nat statistics             --> estadísticas sobre el uso del NAT
Router# debug ip nat                       --> se muestra cuando se está aplican do NAT
Router# clear ip nat translation *         --> borra las entradas dinámicas de la tabla NAT
```

4.4 Realización de la práctica

4.4.1 Práctica

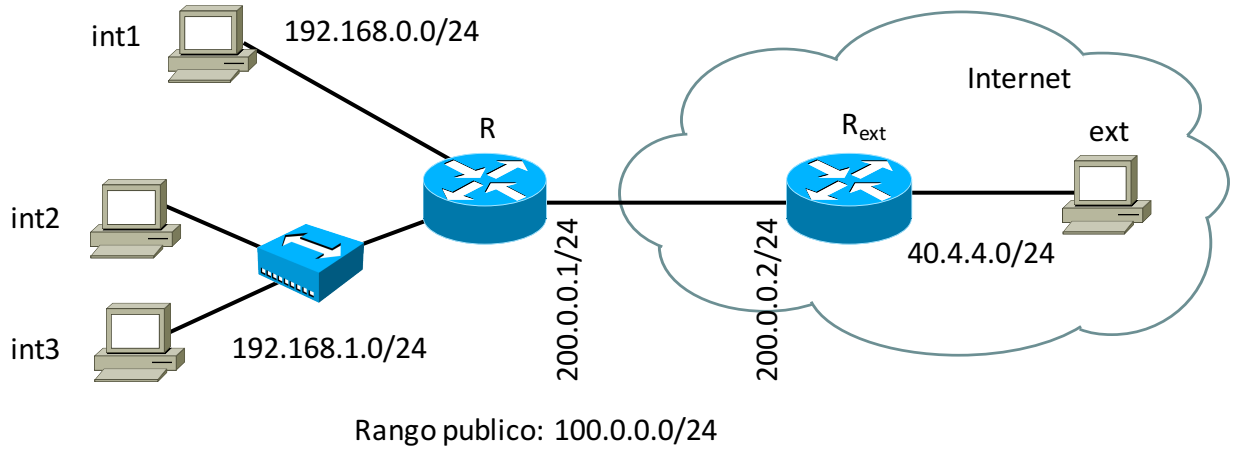

Figura 26: Configuración de la práctica.

La Figura 26 representa la red de esta primera parte. Notar que hay que configurar dos redes internas (192.168.0.0/24 y 192.168.1.0/24, ambas privadas), una red que interconecta el router interno a "Internet" representado por el router Rext y PC externo ext.

Los pasos a seguir son los siguientes:

1. Elegir los dispositivos en Packet Tracer y conectarlos como en la figura. Añadir una interfaz al router R.
2. Configurar los PC internos con una ruta por defecto. Configurar el router R con una ruta por defecto al router Rext para que las redes privadas puedan conectarse a Internet.
3. Configurar el PC externo con una ruta por defecto a Rext
4. Configurar el router Rext con una ruta hacia 100.0.0.0/24 pasando por el gateway 200.0.0.1. Notar que para representar el funcionamiento de Internt se usa un router que no tiene conocimiento de las direcciones privadas pero conoce el rango de direcciones publicas reservadas por la red privada que es 100.0.0.0/24.
5. Comprueba que hay conectividad entre los PC internos pero no con el externo.
6. Configura NAT estático en el router para que int1 sea accesible desde Internet con la dirección pública 100.0.0.100.
    a. Comprueba que int1 puede acceder a ext y viceversa.
    b. Comprueba que int2 y int3 no tienen acceso a ext.
    c. Comprueba la tabla NAT (show ip nat translations)
    d. Comprueba el funcionamiento de NAT con debug ip nat (ejecuta no debug ip nat para desactivar el comando)
7. Configura NAT dinámico con un rango de direcciones públicas (100.0.0.1 – 100.0.0.2).
    a. Comprueba que int1, int2 y int3 tienen acceso a ext.
    b. Comprueba la tabla NAT (show ip nat translations)
8. Elimina el punto 7 y configura PAT para que todos los hosts de la red interna accedan a Internet con la dirección pública de la interface del router (200.0.0.1)
    a. Comprueba que int2 y int3 pueden acceder a Internet.
    b. Comprueba la tabla NAT (show ip nat translations)
    c. Comprueba el funcionamiento de NAT con debug ip nat
    d. Comprueba que ext no puede acceder a int2 y int3 pero si a int1.

4.4.2 Entrega

Según el plazo marcado, entragar un informe con nombre y apellido y rellenando la plantilla de esta practica 3 disponible en la sección de entregas de la Intranet.

Lab. 5 – Configuración de cortafuegos

5.1 Objetivo de la práctica

El objetivo de esta práctiva es familizarizarse con la configuración de fireall y saber configurar un router mediante listas de acceso (ACL).

5.2 Access List (ACL)

5.2.1 Introducción

Las listas de acceso (ACL) se usan para el filtrado de paquetes en función de ciertos parámetros como pueden ser las direcciones de red origen o destino, los puertos origen o destino, el tipo de protocolo (ip, icmp, tcp, udp, etc). Una de las aplicaciones donde se usan más las listas de acceso es en la seguridad de la red. Con las ACLs se puede bloquear el tráfico no deseado en una interfaz ya sea de salida o de entrada. Las ACLs no sólo se usan en temas de seguridad, sino que también para identificar paquetes en aplicaciones como NAT (Network Address Translation), en protocolos de encaminamiento como BGP, etc.

Existen ACLs para distintas pilas de protocolos: TCP/IP, IPX/SPX, AppleTalk, etc. Este documento se centra en las ACLs aplicadas a seguridad en la red para TCP/IP. Capa protocolo tiene asignado un rango de ACLs. Por ejemplo las ACLs entre la 1 y la 199 se usan en TCP/IP, mientras que las comprendidas entre la 800 y la 999 se usan para IPX/SPX, otros rangos se usan para DECnet (300-399), XNS (400-599), AppleTalk (600-699), etc.

Cuando se crea una ACL y se aplica a una interfaz, se está creando una secuencia de instrucciones que son chequeadas cada vez que un paquete entra o sale por esa interfaz. Es importante notar varias características de las ACLs.

Primero, que una ACL se aplica a la interfaz ya sea de entrada o de salida. Se pueden crear una ACL para la interfaz de salida y otra distinta para esa interfaz de entrada. No se pueden crear varias ACL aplicadas a la misma interfaz en un mismo sentido.

Lo segundo, las ACLs son secuencias de instrucciones que son chequeadas contra el paquete. El orden de las instrucciones es importante, ya que cuando una línea de la secuencia da cierta en el chequeo, se toma una acción y se sale de la ACL, es decir no se continua chequeando para comprobar que haya otra línea de la secuencia que también resulta cierta. Por consiguiente es muy importante diseñar la ACL en la secuencia que nos interese más.

Por ejemplo no es lo mismo estas dos líneas de una ACL:

- Si el paquete es icmp recházalo
- Si el paquete es ip acéptalo

que la secuencia:

- Si el paquete es ip acéptalo
- Si el paquete es icmp recházalo

Suponed que llegara un paquete ICMP. En el primer caso el paquete se rechazaría ya que la primera línea se cumple, el paquete es ICMP. En el segundo caso el paquete ICMP se aceptaría ya que la primera línea también se cumple, con lo cual ya no se comprobaría la segunda.

Otro aspecto importante es que no podemos insertar líneas en la secuencia. Si nos equivocamos al crearla o queremos insertar una línea a hay que borrar las líneas hasta el punto de inserción.

Finalmente, también **muy importante**, la última línea de una lista de acceso **nunca** aparece, es decir existe de forma explicita y siempre es **deniega todo**.

Dentro de las listas de acceso TCP/IP hay dos tipos de ACLs

- Listas de acceso IP estándar (1-99)
- Listas de acceso IP extendidas (100-199)

5.2.2 Wildcard

La wildcard es una mascara de 32 bits que indica que bits de la dirección IP se tienen que comprobar y cuales no. Si los bits de la máscara están a 0 entonces se comprueban, si están a 1 entonces no se comprueban.

Por ejemplo si queremos que un paquete que entra se compruebe si pertenece al host con dirección IP 145.34.5.6, queremos que se comprueben todos los bits de la dirección IP. Eso significa que la wildcard mask sería 0.0.0.0. En este caso se suele sustituir la tupla @IP wildcard por host @IP. Por ejemplo la tupla 145.34.5.6 0.0.0.0 se puede expresar como host 145.34.5.6.

Si quisiéramos que no se comprobase ningún bit, pondríamos una wildcard mask de 255.255.255.255. en este caso se suele sustituir la tupla @IP WildcardMask por any. Por ejemplo la tupla 145.34.5.6 255.255.255.255 se puede expresar como any.

También podemos expresar redes. Por ejemplo para comprobar todos los paquetes que vengan de la red 145.34.5.0/24. Eso significa que tenemos que comprobar todos los paquetes cuyos primeros 24 bitscoincidan con los de la dirección de red. Luego la wildcard mask debería ser 0.0.0.255.

5.2.3 ACL estándar

Las ACLs estándar solo usan las direcciones origen para hacer la comprobación. Las listas de acceso estándar tienen números (acl#) comprendidos entre el 1 y el 99. El comando tiene el siguiente formato:

```
Router# configure terminal
Router(config)# access-list #ACL {deny|permit} {host @IPorigen | @IPorigen Wildcard | any}
```

El commando access-list crea la lista de acceso con número #ACL y con condición deniego (deny) o permito (permit) sobre la dirección IP origen especificada. La @IP origen puede ser:

- una @IP concreta y se pone host @IP
- una conjunto de @IP como puede ser una red; en este caso se usa la wildcard y se pone @IP wildcard
- puede ser cualquier @IP y se pone **any**

Recordad que la última línea de una ACL nunca aparece pero siempre es "access-list #ACL deny any".

Una vez creada la lista de acceso hay que aplicarla a una interfaz de un router en un sentido concreto. Una ACL se suele aplicar lo más próximo posible a la zona que se quiere proteger. El comando es:

```
Router# configure terminal
Router(config)# interface interfaz
Router(config-if)# ip access-group #ACL {in|out}
```

Una vez creada, una ACL no se puede modificar. Lo único que se puede hacer es añadir más lineas si se quiere controlar otros tipos de paquetes. Si hay algún error, la única solución posible es borra la ACL entera y volver a crearla. Para borrar una ACL se ejecuta el comando:

```
Router(config)# no access-list #ACL
```

Para eliminar la aplicación de una ACL a una interfaz se ejecuta el comando:

```
Router(config-if)# no ip access-group #ACL {in|out}
```

5.2.4 ACL extendida

Las ACLs extendidas permiten usar tanto las direcciones origen como destino para hacer la comprobación. Además permiten especificar el protocolo sobre el que se quiere hacer la comprobación y en el caso de que sea TCP o UDP especificar el puerto. Las listas de acceso extendidas tienen números (acl#) comprendidos entre el 100 y el 199. El comando tiene el siguiente formato:

```
Router# configure terminal
Router(config)# access-list #ACL {deny|permit} protocol {host @IPorigen | @IPorigen Wildcard | any}
[operador PuertoOrigen] {host @IPdestino | @IPdestino Wildcard | any} [operador PuertoDestino]
[established]
```

El comando *access-list* crea

- la lista de acceso extendida con número #ACL
- con condición deniego (deny) o permito (permit)
- de un determinado protocol que puede ser IP, TCP, UDP, ICMP, etc.
- sobre una dirección IP origen concreta (host @IPorigen), un grupo de direcciones (@IPorigen Wildacard) o todas las @IP (any) con determinados puertos origenes usando un operador que puede ser **lt, gt, eq, neq** (less than, greater than, equal, non equal) a un puerto determinado (PueroOrigen)
- y/o sobre una dirección IP destino concreta (host @IPdestino), un grupo de direcciones (@IPdestino Wildacard) o todas las @IP (any) con determinados puertos origenes usando un operador que puede ser **{lt, gt, eq, neq}** a un puerto determinado (PueroDestino)
- y finalmente established se usa para controlas tráfico TCP perteneciente a una conexión establecida de forma que cuando se pone en la lista de acceso solo permite paquetes que son respuestas de una petición de conexión en sentido contrario. Es decir cuando se pone se controlan (denegar o permitir) solo las respuestas.

Recordad que en el momento que se crea una ACL, la última línea nunca aparece pero siempre denega todo con "access-list #ACL deny ip any any".

Como en el caso de ACL estandar, tambien en este caso una vez creada hay que aplicar la ACL a una interfaz de un router en un sentido concreto. El comando es:

```
Router# configure terminal
Router(config)# interface interfaz
Router(config-if)# ip access-group #ACL {in|out}
```

5.2.5 Verificación

```
Router# show access-list        --> muestra las ACLs definidas
Router# show running-config     --> muestra la configuración del router y por lo tanto de las ACL
```

5.3 Ejemplos

Considerar el ejemplo de la Figura 27.

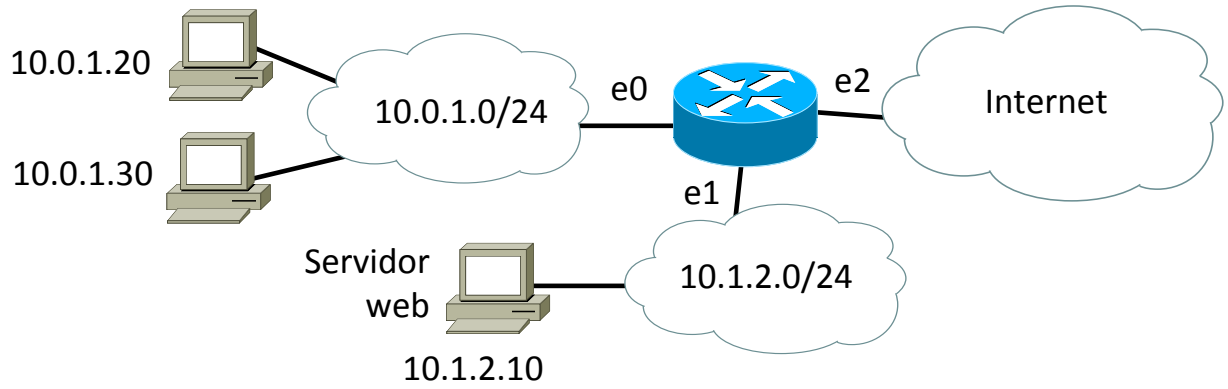

Figura 27: Ejemplo.

5.3.1 Ejemplo 1

En este primer ejemplo suponer que de la red 10.0.1.0 solo se quiere pemitir el acceso a Internet a los hosts 10.0.1.20 y 10.0.1.30.

En este caso una ACL estándar es suficiente ya que interesa solo controlar la @IP origen. Por lo tanto la ACL es

```
Router# configure terminal
Router(config)# access-list 1 permit host 10.0.1.20
Router(config)# access-list 1 permit host 10.0.1.30
```

Estas dos líneas son suficientes ya que hay que recordar que en el momento de crear una ACL ya se configura en automatico una última línea que deniega todo el resto.

Ahora hay que aplicar la ACL a una interfaz del router en un sentido concreto. La regla es aplicar la ACL a la interfaz más próxima a la zona que se quiere controlar. En este caso es la interfaz e0 y el sentido es de entrada respecto al router. De hecho con esta lista de acceso creada, la interfaz e0 es la única interfaz posible, ya que si se aplicara a la interfaz e2, también pasarían por esta interfaz los paquetes que vienen de la red 10.1.2.0/24 y quedarían descartado.

Por lo tanto el comando para aplicar la ACL es

```
Router# configure terminal
Router(config)# interface e0
Router(config-if)# ip access-group 1 in
```

5.3.2 Ejemplo 2

En este segundo ejemplo suponer que se quiere controlar el acceso a la red 10.1.2.0. En concreto se quiere permitir que desde Internet y de la red interna solo se pueda acceder al servicio web (puerto 80 del TCP) del servidor 10.1.2.10 y denegar cualquier otro paquete.

En este caso hay que usar una ACL extendida ya que se quieren controlar más parámetros. La ACL es

```
Router# configure terminal
Router(config)# access-list 100 permit TCP any gt 1023 host 10.1.2.10 eq 80
```

Este comando crea

- una ACL número 100 (extendida),
- que controla que el protocolo sea TCP,
- que el origen sea cualquiera (any) y que estas orígenes tengan un puerto más grande de 1023 (gt 1023) ya que deben ser clientes del servidor
- que el destino sea en concreto el host 10.1.2.10 y que el puerto destino sea igual a 80 (eq 80) ya que es el puerto que identifica un servidor web.

Considerando que la última línea oculta denega todo el resto, esta línea es suficiente.

Ahora hay que aplicar la ACL a una interfaz del router en un sentido concreto. En este caso conviene aplicarla a la interfaz e1 y que el sentido sea de salida respecto al router. De salida porque el origen es cualquiera y el destino es el servidor por lo tanto los paquetes deben ir hacía el servidor (sentido de salida de la interfaz e1)

Por lo tanto el comando para aplicar la ACL es

```
Router# configure terminal
Router(config)# interface e1
Router(config-if)# ip access-group 100 out
```

Considerando la configuración anterior, ahora se quiere dar la posibilidad a cualquier host de hacer ping al servidor 10.1.2.10. En este caso, este añadido no va en contra de lo que ya se ha hecho anteriormente, por lo tanto, se puede añadir una línea más a la ACL 100. En este caso para permitir el uso del ping hay que tener en cuenta que ping usa el protocolo ICMP y no se usan puertos. En modo configuración general, el comando es:

```
Router(config)# access-list 100 permit ICMP any host 10.1.2.10
```

Como se puede observar se usa la ACL 100 y se permiten paquetes ICMP con cualquier @IP origen (any) y la @IP destino concreta del host 10.1.2.10. Esta línea no borra la anterior que daba permiso de acceso al servidor de paginas web, simplemente se pone en segundo lugar y el router controlará estas condiciones solo después de haber verificado la anterior. Como la ACL 100 ya se ha aplicado anteriormente a la interfaz e1 en el sentido de salida, no hace falta volver a hacerlo.

5.3.3 Ejemplo 3

Finalmente, en este ejempo suponer que se quiere controlar el acceso de Internet a los usuarios de la red interna 10.0.1.0/24. En concreto se quiere prohibir que usuarios de Internet accedan a la red 10.0.1.0/24 pero hay que permitir que los usuarios de la red interno puedan usar servicios TCP de Internet. Es decir, nadie de Internet puede empezar una comunicación con la red interna, pero si deben poder contestar a peticiones de la red interna. En este caso hay que usar la opción *established* que controla justamente este tipo de acciones.

Hay que usar una ACL extendida

```
Router# configure terminal
Router(config)# access-list 101 permit TCP any lt 1024 10.0.1.0 0.0.0.255 gt 1023 established
```

En concreto este comando crea

- una ACL número 101 (extendida),
- que controla que el protocolo sea TCP,
- que el origen sea cualquiera (any) y que estos orígenes tengan un puerto menor que 1024 (lt 1024) ya que deben ser servidores (es decir los servidores de Intrenet deben poder contestar a los clientes internos).
- que el destino sean los hosts de la red 10.0.1.0 (la wildcard es 0.0.0.255, el inverso de la mascara 255.255.255.0) y que el puerto destino sea mayor que 1023 (gt 1023) ya que deben ser clientes.
- y finalmente established para controlar que sean efectivamente respuesta de servidores a peticiones hechas anteriorermente por los clientes internos.

La última línea oculta denega todo el resto.

La ACL en este caso se aplica a la interfaz e0 en el sentido de salida respecto al router. En este caso conviene aplicarla a la interfaz e0 de salida para controlar que desde Internet se acceda a la 10.0.1.0 según esta ACL.

Por lo tanto, el comando para aplicar la ACL es

```
Router# configure terminal
Router(config)# interface e0
Router(config-if)# ip access-group 101 out
```

5.4 Realización de la práctica

5.4.1 Práctica

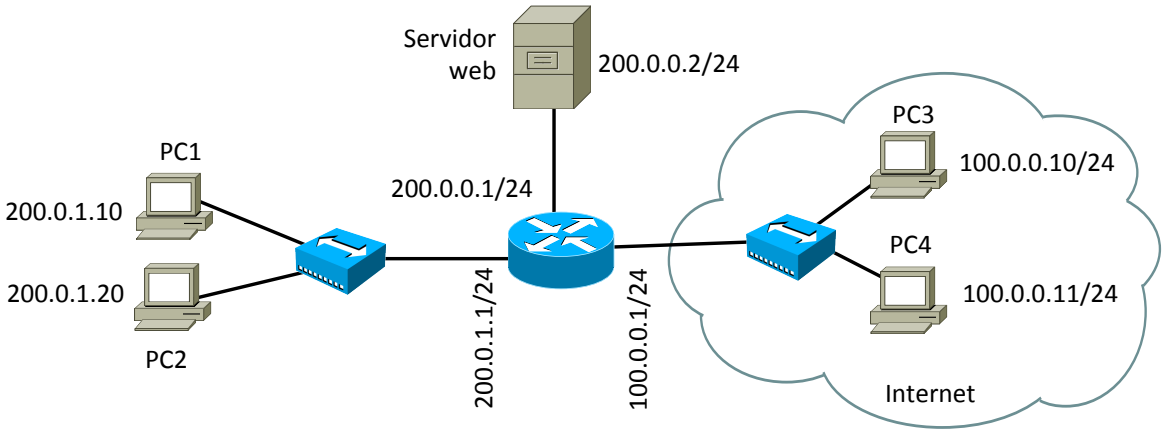

Figura 28: Configuración de la práctica.

La Figura 28 representa la red de esta práctica. En esta práctica se supone que hay dos PCs internos a una red, un Servidor web en una red DMZ y luego para emular un cualquier host de Internet se usan PC3 y PC4.

Los pasos a seguir son los siguientes:

1. Elegir los dispositivos en Packet Tracer y conectarlos como en la figura. Añadir una interfaz al router.
2. Configurar las @IP de las 3 interfaces del router.
3. Configurar las @IP de todos los PCs y configurar una ruta por defecto hacía el router.
4. Configurar la @IP del Servidor web, una ruta por defecto hacía el router y el servicio web así como se explica en el Anexo B al final de este documento. El Servidor web no es nada más que un PC normal (con su @IP y tabla de encaminamiento) solo que además tiene una aplicación servidor que proporciona permite a los clientes ver una página web.
5. Comprueba que hay conectividad entre todos los PCs y que todos los PCs pueden acceder a las páginas web del servidor.
6. Configurar una ACL de forma que solo PC1 pueda acceder a Internet y al Servidor web (fijarse en el Ejemplo 1).
    a. Comprueba que PC1 puede hacer ping a cualquier otro PC, incluido el Servidor web.
    b. Comprueba que PC1, a través de su web browser (ver Anexo B), puede ver la web del Servidor.
    c. Comprueba que PC2 no puede hacer ping a PC3 o PC4 y tampoco puede ver la web del Servidor.
    d. ¿PC2 puede hacer ping a PC1? ¿Por qué?
    e. Comprueba que PC3 y PC4 pueden hacer ping a PC1 y pueden ver la web del Servidor.
7. Configurar una ACL de forma que solo se pueda acceder al servicio web del Servidor y solo PC1 puede hacer ping al Servidor (fijarse en el Ejemplo 2).
    a. Comprueba que PC1, PC3 y PC4 pueden ver la web del Servidor. Debe verse la página por defecto del servidor (ver Anexo B). Si hay algún error, la página en el web browser se queda en blanco.
    b. ¿PC2 puede ver la web del Servidor? ¿Por qué?
    c. Comprueba que PC1 puede hacer ping al Servidor y los demás no.

5.4.2 Entrega

La entrega de esta práctica es voluntaria, en el sentido que no es obligatoria y solamente sumará puntos para los que decidan entregarla.

Según el plazo marcado, entragar un informe con nombre y apellido y rellenando la plantilla de esta practica 3 disponible en la sección de entregas de la Intranet.

Anexo A – Simulador GNS3

GNS3 es otra herramienta que se podría usar para configurar redes. En concreto GNS3 es un simulador grafico de redes (http://www.gns3.net/) de código abierto y libre distribución que se puede utilizar en múltiples sistemas operativos, incluyendo Windows, Linux y MacOS X. En particular, permite crear redes a través de un entorno grafico usando dispositivos de red que emulan CISCO IOS y Juniper JunOS.

GNS3 es una excelente herramienta complementaria a los laboratorios de red. También se puede utilizar para experimentar o verificar las configuraciones de equipos de red antes de implementarlo más adelante en routers reales.

Actualmente su versión más estable es la 0.7.4. La versión "all-in-one" proporciona todas las herramientas útiles para el simulador excepto los sistemas operativos a simular como CISCO IOS, JunOS, etc. Estos sistemas operativos no son de libre distribución y el usuario de GNS3 debe proporcionar las imagenes de los sistemas operativos que necesita simular.

A continuación se ilustran algunos ejemplos.

La Figura 29 muestra un ejemplo de red creada a partir del entorno grafico de GNS3. El menu de selección de los dispositivos disponibles se encuentra en la ventana de la izquierda. Una vez arrastrados en la ventana central, estos dispositivos se pueden conectar entre si a través de enlaces que pueden usar tecnologias distintas, bien fastethernet, gigabitethernet, serial, etc.

La Figura 30 muestra como se puede acceder a la consola de un router. El router es realmente emulado, así que está corriendo realmente el sistema operativo del router y lo que aparece es la consola para configurarlo. Como las imagenes de los sistemas operativos son las reales, los comandos de configuración son exactamente iguales a los de un dispositivo real.

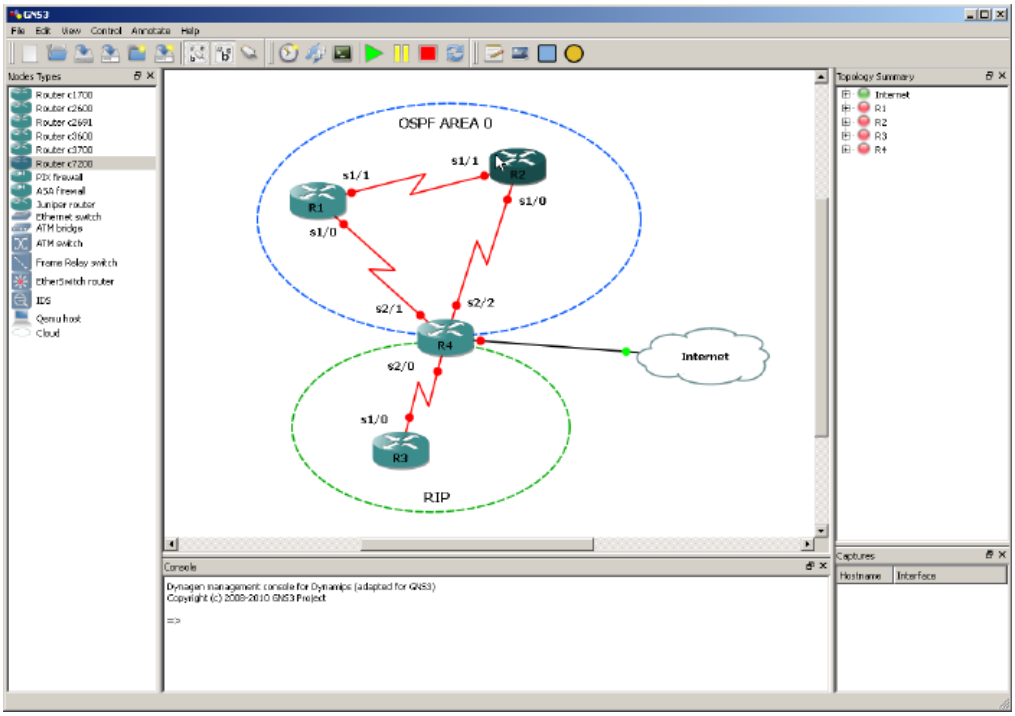

Figura 29: GNS3 permite crear redes a través de un entorno grafico.

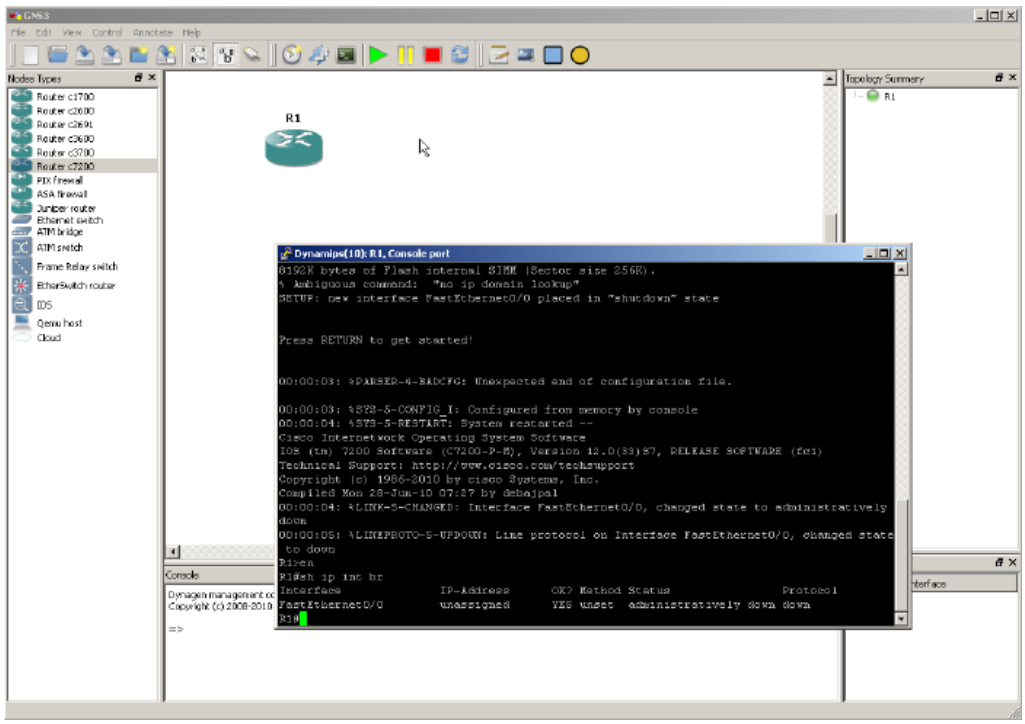

Figura 30: Acceso a la consola de configuración del router R1.

Anexo B – Configuración de un servidor web en Packet Tracer

Packet Tracer permite configurar servidores. En este anexo se explica brevemente como configurar un servidor web.

La primera operación es seleccionar un servidor genérico en los iconos de dispositivos. El servidor se encuentra en el apartado End Devices y es el tercer icono (Figura 31).

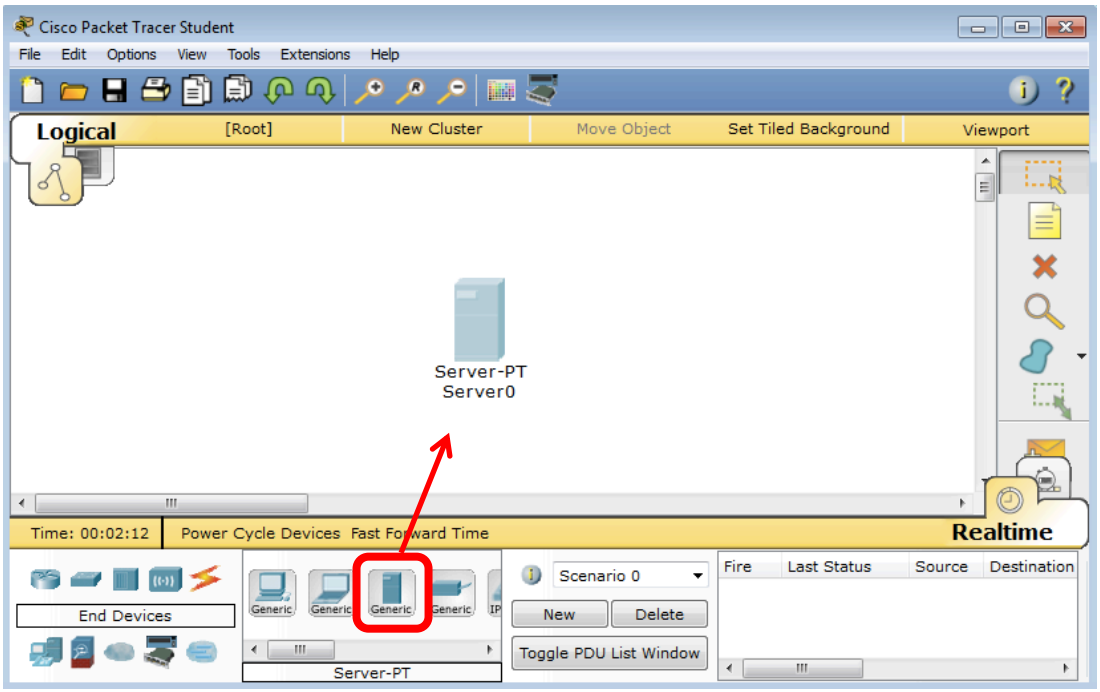

Figura 31: Selección de un servidor.

Por defecto este servidor es un servidor HTTP (es decir un servidor web). Clicando en el servidor aparece una nueva ventana y en el apartado Services se pueden ver los servicios que se puede activar y gestionar (Figura 32). Por ejemplo se puede configurar el servidor para que sea un servidor HTTP, pero también DHCP, DNS, email, ftp, etc.

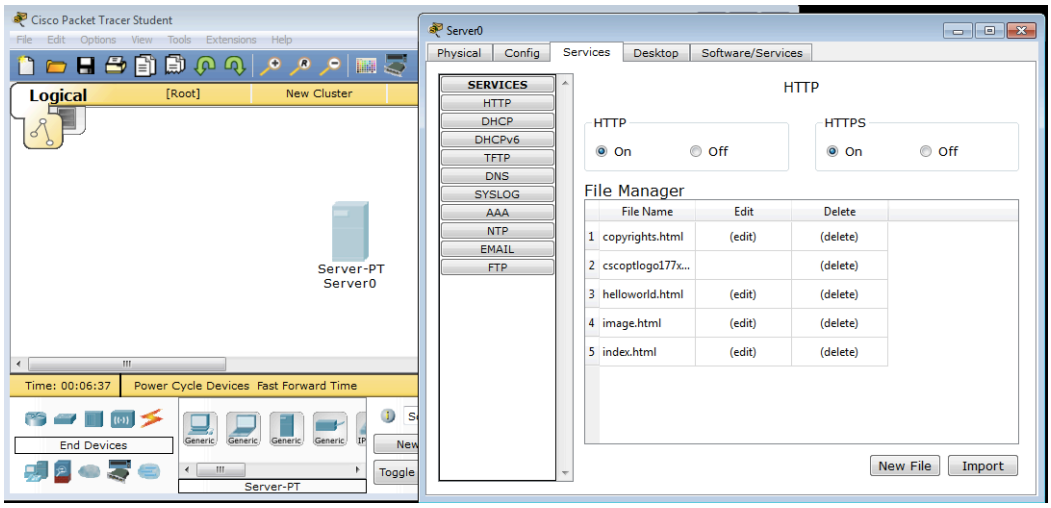

Figura 32: Servicios disponibles.

Como se puede ver en la Figura 32, el servicio HTTP (y HTTP seguro, HTTPS) está activo (donde pone HTTP on). En esta ventana además se pueden editar y crear paginas web en HTML. Por defecto ya vienen 5 páginas ya creadas, donde la principal, es decir la que sale primero al conectarse al servidor es index.html (la última).

Para verificar que el servicio funciona y se puede consultar la página web de este servidor, se configura la siguiente red muy simple. Esta red se ilustra en la Figura 33. Se ha configurado el servidor con la @IP 200.0.0.1 y el cliente con la @IP 200.0.0.2 de la misma forma que se explica en Lab.1.

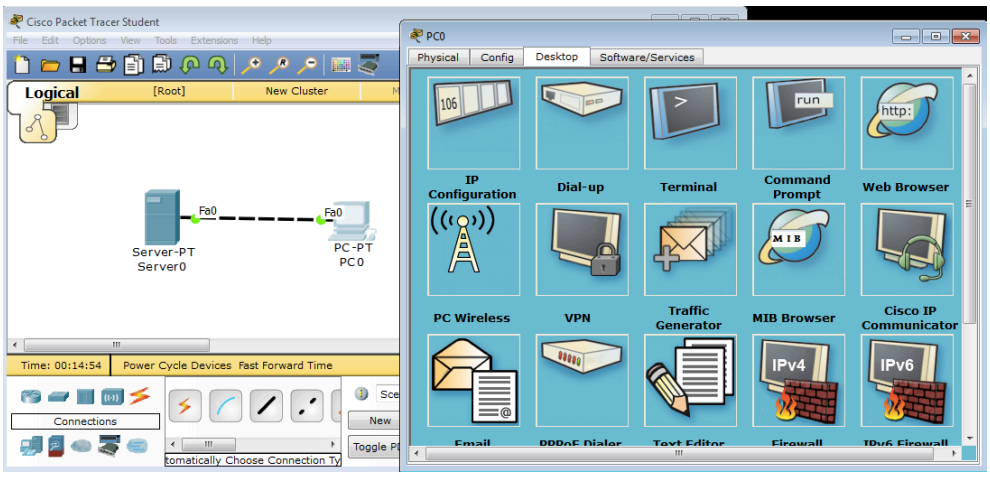

Figura 33: Red simple para verificar el correcto funcionamiento del servidor.

Ahora que la red está configurada, se puede verificar que el cliente (PC-PT PC0) puede ver la pagina web del servidor. En el apartado Desktop del cliente hay que darle al icono Web Browser y se abrirá un navegador muy simple. Donde pone URL se pone la @IP del servidor, en este caso 200.0.0.1. Hay que fijarse que no hay ningún servicio DNS disponible en esta red, por lo tanto no se pueden usar nombre y hay que usar las direcciones IP como destinos.

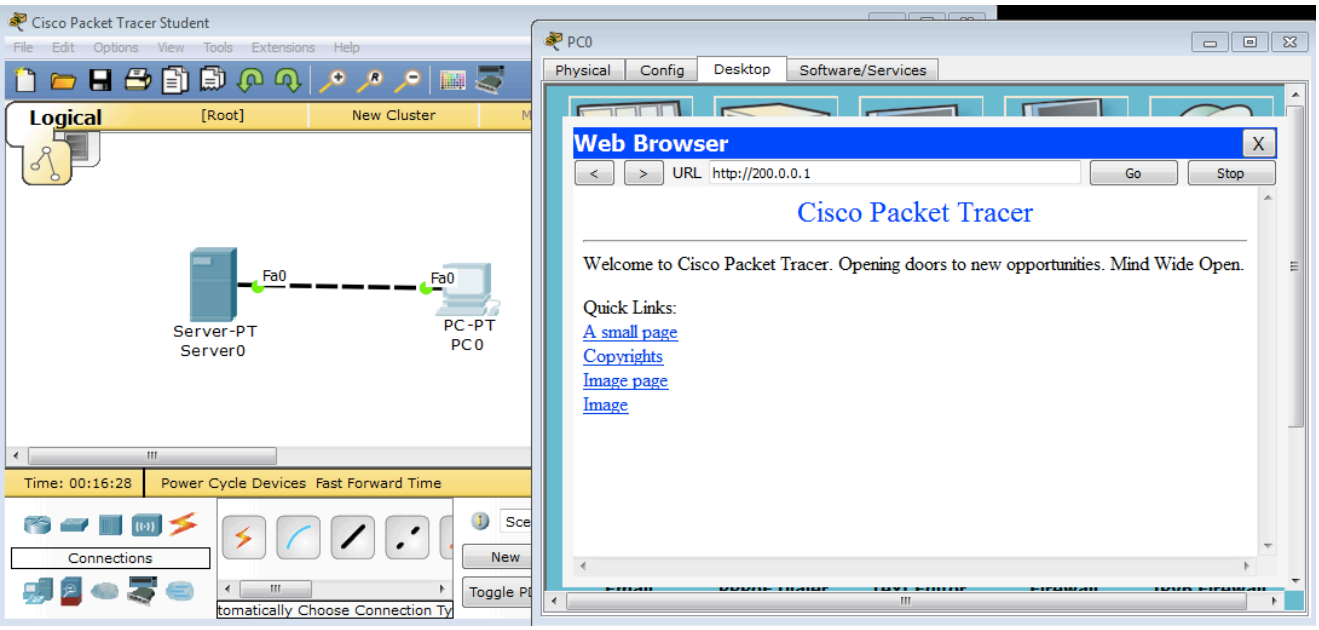

Figura 34: Verificación del correcto funcionamiento del servidor web.

En la Figura 34 se puede ver que el cliente puede conectarse al servidor y ver las paginas webs disponibles. La principal como se decía es la index.html que simplemente tiene un titulo (Cisco Packet Tracer) y un texto con 4 enlaces a las otras 4 paginas disponibles. Si hay algún error, al probar a conectarse a la web del servidor, la página se quedaría en blanco.