

Práctica 1

Nivel de Red

Descripción de la práctica

La práctica consiste en aplicar los conocimientos adquiridos en la asignatura con respecto al Nivel de Red, y otros protocolos relacionados. El objetivo de la práctica es que el estudiante sea capaz de definir un plan de direccionamiento y aplicarlo a un escenario concreto. El estudiante deberá configurar equipos finales, así como routers y otros servicios de red. Además, el estudiante comprobará el funcionamiento del nivel de red durante el proceso, y deberá ser capaz de solucionar problemas típicos que afectan a dicho nivel.

La práctica se realizará en un entorno simulado en el que el estudiante creará los escenarios solicitados, configurando los equipos y comprobando su funcionamiento.

Dicho entorno permite introducir de forma sencilla equipos finales, tanto equipos de usuario como servidores DNS, WEB, etc, y configurarlos. Además, el entorno permite añadir a la topología dispositivos de red, como routers (o switches, cuya gestión se realizará en la Práctica 2). Estos elementos de red se configurarán utilizando la interfaz de línea de comandos (CLI) del IOS de Cisco, puesto que los routers y switches son equipamiento real Cisco simulado. Junto con este enunciado se proporciona una [guía de uso del simulador](#) utilizado (Packet Tracer) y una [hoja de referencia rápida](#) con los comandos a utilizar.

Normas y entrega

La práctica se realiza en grupos de dos personas, que pueden ser propuestos por los propios estudiantes o establecidos por los profesores en caso de no disponer de compañero.

Antes de la realización de la práctica, los estudiantes deberán haber leído y comprendido este enunciado, así como la [guía de uso del simulador](#) utilizado (Packet Tracer).

El primero de los supuestos (apartado 0) es teórico y debe ser realizado **antes de iniciar la configuración en el simulador**. Para ello, se pone a disposición del estudiante el siguiente [formulario inicial](#) donde deberá reflejar la solución del direccionamiento realizado para este apartado 0.

Adicionalmente, se pone a disposición de los estudiantes otro [formulario final](#), donde los estudiantes deberán reflejar la solución dada a los distintos apartados de la práctica.

La entrega de la práctica consistirá en la entrega de los siguientes 3 ficheros en la tarea de Moodle habilitada para tal efecto:

- **Formulario inicial:** el [formulario inicial](#) con la solución del apartado 0.
- **Formulario final:** el [formulario final](#) con la solución a los distintos apartados de la práctica.
- **Fichero .pkt:** fichero .pkt (simulador) con la solución de la práctica.

Aunque la práctica se puede realizar en grupos de dos estudiantes, **ambos estudiantes deberán realizar la entrega de los tres ficheros forma individual en la tarea de Moodle** (indicando en los formularios los integrantes del grupo). **Solo aquellos estudiantes que hayan realizado la entrega de los 3 ficheros podrán presentarse al examen de la práctica.**

Evaluación de la práctica

El objetivo final de la práctica es familiarizar al estudiante con un entorno de red real, adquiriendo habilidades prácticas con respecto a la configuración de las redes empresariales y la resolución de problemas.

Para que el estudiante compruebe su grado de adquisición de conocimientos, tendrá a su disposición un formulario de autoevaluación que deberá responder con datos y habilidades obtenidas en el laboratorio.

El estudiante deberá realizar, en la fecha que se indique, un examen sobre la práctica, que certifique su nivel de adquisición de los conocimientos teóricos y prácticos empleados en la misma. Este examen es individual.

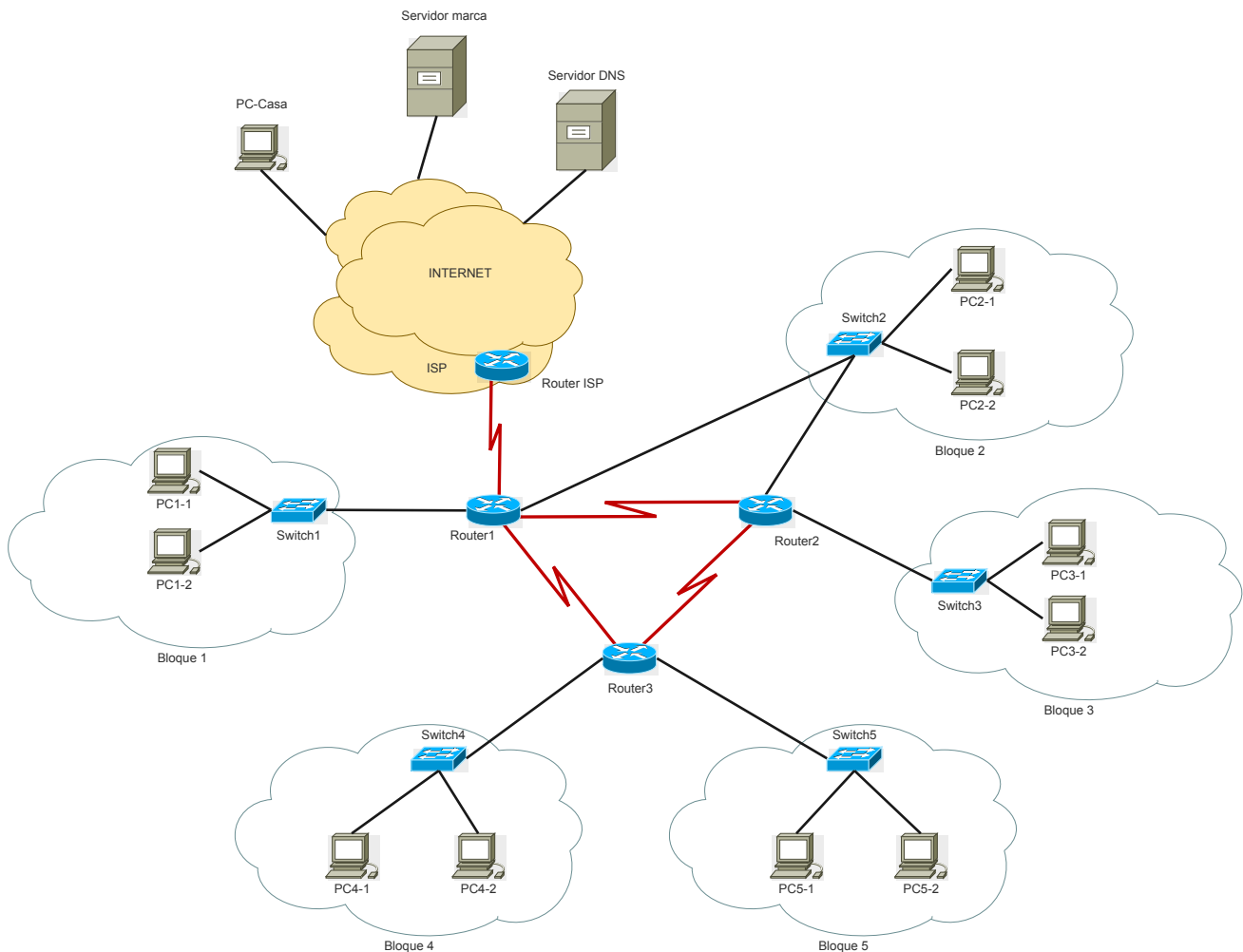


La evaluación de la práctica consiste en la evaluación de los conceptos que se practican en la misma (planes de direccionamiento, dominios de difusión, configuración de equipos finales, rutas, comportamiento de un router, NAT, etc). La **comprensión y aplicación** de dichos conceptos constituye la evaluación de la práctica, y no su mera realización.

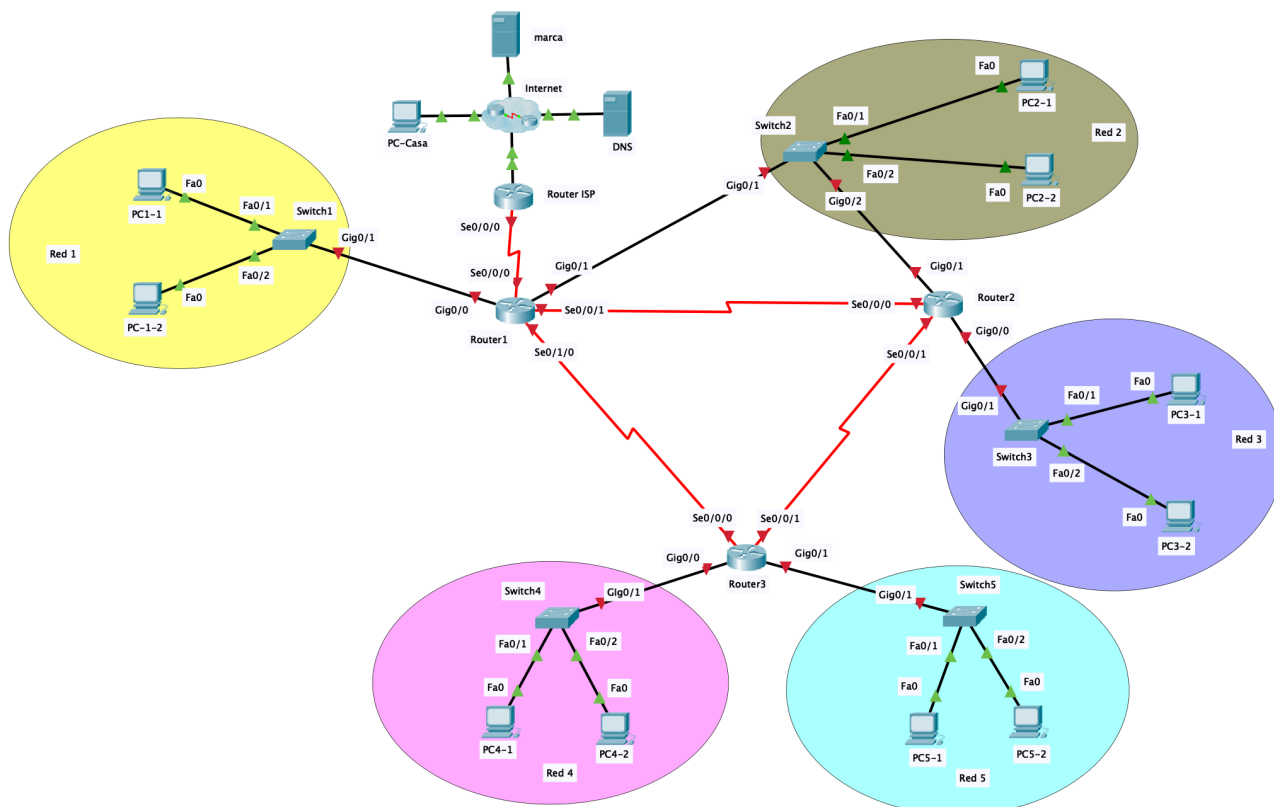
Escenario

Una universidad dispone de 5 edificios y ha desplegado una topología de red formada por 3 routers, una subred por edificio más los enlaces necesarios. El Router **Router1** ofrece acceso a Internet a través de un operador **ISP**.

El **Router1** tiene conectadas las subredes de los bloques **Bloque1** y **Bloque2** (i.e. **RED 1** y **RED 2**). El **Router2** por su parte tiene conectadas las subredes de los bloques **Bloque2** y **Bloque3** (i.e. **RED 2** y **RED 3**). Finalmente, el **Router3** está conectado a las subredes del **Bloque4** y **Bloque5** (i.e. **RED 4** y **RED 5**). Todos los routers están conectados entre ellos (i.e. El **Router1** con los routers 2 y 3, El **Router2** con los routers 1 y 3, etc.). Finalmente el **Router1** se conecta con el router del ISP para acceder a Internet.



El **Router1** emplea NAT con puerto (también llamado NATP o PAT) para la traducción de las direcciones privadas empleadas en la red de la universidad. La configuración de NATP ya está realizada y no es necesario modificarla hasta que se indique específicamente.



La topología física se modificará en función del número de matrícula más baja de los estudiantes del grupo. Para ello se empleará el formulario que acompaña a este enunciado.

0. Plan de direccionamiento

El ISP le ha asignado a la universidad una única dirección IP pública, por lo que su Centro de Cálculo ha decidido utilizar parte del rango privado de direcciones de clase A para asignarlas a las diferentes subredes internas.

La primera tarea, que deberá realizarse **antes de acudir al laboratorio**, es la de crear el plan de direccionamiento de la universidad en el **formulario** que acompaña a este enunciado. Dicho formulario contiene las tablas con los requisitos de dimensionamiento de las diferentes redes, y deberán ser completadas por los estudiantes incluyendo **TODAS** las redes presentes en la topología, y las direcciones IP, máscara y Gateway (en su caso) de los equipos.

Los tamaños de cada red se determinarán al cumplimentar el formulario adjunto, en función del número de matrícula más bajo de los dos estudiantes del grupo.



Estas tablas, en papel, se entregarán al entrar al laboratorio, y es condición indispensable para acceder al mismo. Así mismo, se recomienda llevar otra copia para realizar la práctica.

Se utilizarán direcciones privadas del rango **172.16.0.0/16**. De hecho las direcciones a asignar comienzan en la dirección **172.16.0.0**. Se deberán dimensionar subredes necesarias, en orden de la **RED 1** a la **RED 5**, partiendo de dicha dirección (**172.16.0.0**) y sin dejar huecos innecesarios entre subredes. Las direcciones asignadas a cada subred siempre partirán desde la última

dirección posible en la subred anterior. Las subredes deben ser capaces de alojar el número de equipos que se indica en la primera tabla del formulario.



La tabla de redes se deberá completar añadiendo TODAS las redes internas a la universidad necesarias para su funcionamiento (líneas con puntos suspensivos). Estas redes emplearán direcciones IP empezando en la dirección **192.168.1.0** . Empiece asignando las redes que conecten los routers con la numeración más baja.

También se deberá completar el resto de la información requerida en la tabla con la red pública, que ya está creada, a partir de las direcciones IP de los equipos.



La direcciones de red del **Enlace Público** del **Router1** se ha de obtener, teniendo en cuenta la dirección del siguiente salto (**138.10.0.1/30**).

A continuación se deberán seleccionar los parámetros necesarios de la configuración TCP/IP para configurar los equipos finales y los routers de la práctica. Las direcciones ya configuradas, que aparecen en las tablas, no se pueden modificar. Para asignar direcciones, aplique las siguientes indicaciones:

- En las redes en las que haya un sólo router, asigne a dicho router **la última dirección IP del rango** que se pueda utilizar.
- En las redes en las que haya dos routers, **el router con numeración mayor utiliza la dirección más alta** (por ejemplo, **Router3** > **Router1**)
- Asigne direcciones IP **estáticas** a los equipos, **comenzando por el extremo inferior del rango**.

Utilice la topología detallada del escenario o el propio fichero **.pkt** proporcionado para identificar las interfaces de los routers que los conectan a las diferentes redes.

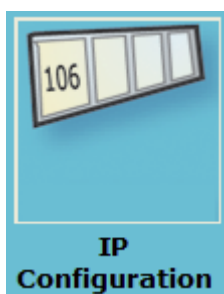
Finalmente, se deberán definir las tablas de rutas para los routers **Router1** , **Router2** y **Router3** . Se deberán crear entradas para poder acceder a todos los equipos de la topología, incluyendo rutas por omisión para salir hacia Internet.



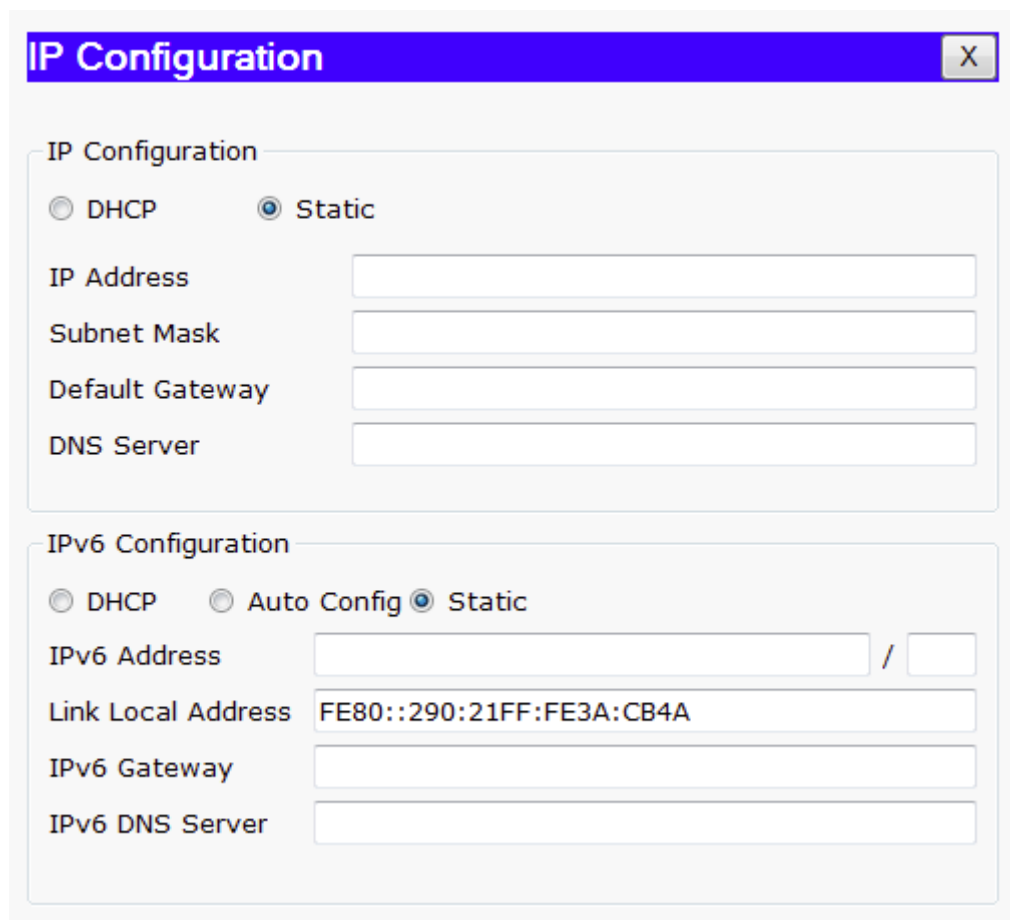
Añada una nota en el fichero **.pkt** con la asignación de direcciones IP y máscaras a las distintas subredes.

1. Configuración TCP/IP de los equipos finales de las subredes de los Bloques

Para los PCs, el direccionamiento es estático en función del plan de direccionamiento realizado. La configuración TCP/IP se realiza a través de su panel de gestión. Haga click en un PC y, en la ventana que se despliega, utilice la pestaña *desktop*. En esta pestaña aparecen herramientas que nos permiten simular el uso real del equipo. La primera de ellas es la que permite realizar la configuración IP:



Configure su dirección IP, máscara, dirección de *gateway* por omisión y dirección del servidor DNS público, tal y como se muestra en la siguiente figura. Utilice para ello las direcciones que calculó en el plan de direccionamiento. Ignore los apartados para IPv6.



IP Configuration

☐ DHCP ☒ Static

IP Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address

IPv6 Gateway

IPv6 DNS Server



Asegúrese de haber configurado correctamente **todos** los equipos finales.

Escoja un PC cualquiera, y obtenga su configuración a través de su interfaz de mandatos o



command prompt. Observe la salida del mandato `ipconfig`, que es la herramienta Windows para mostrar la configuración de las interfaces de red de un equipo.

2. Prueba de la conectividad (1)



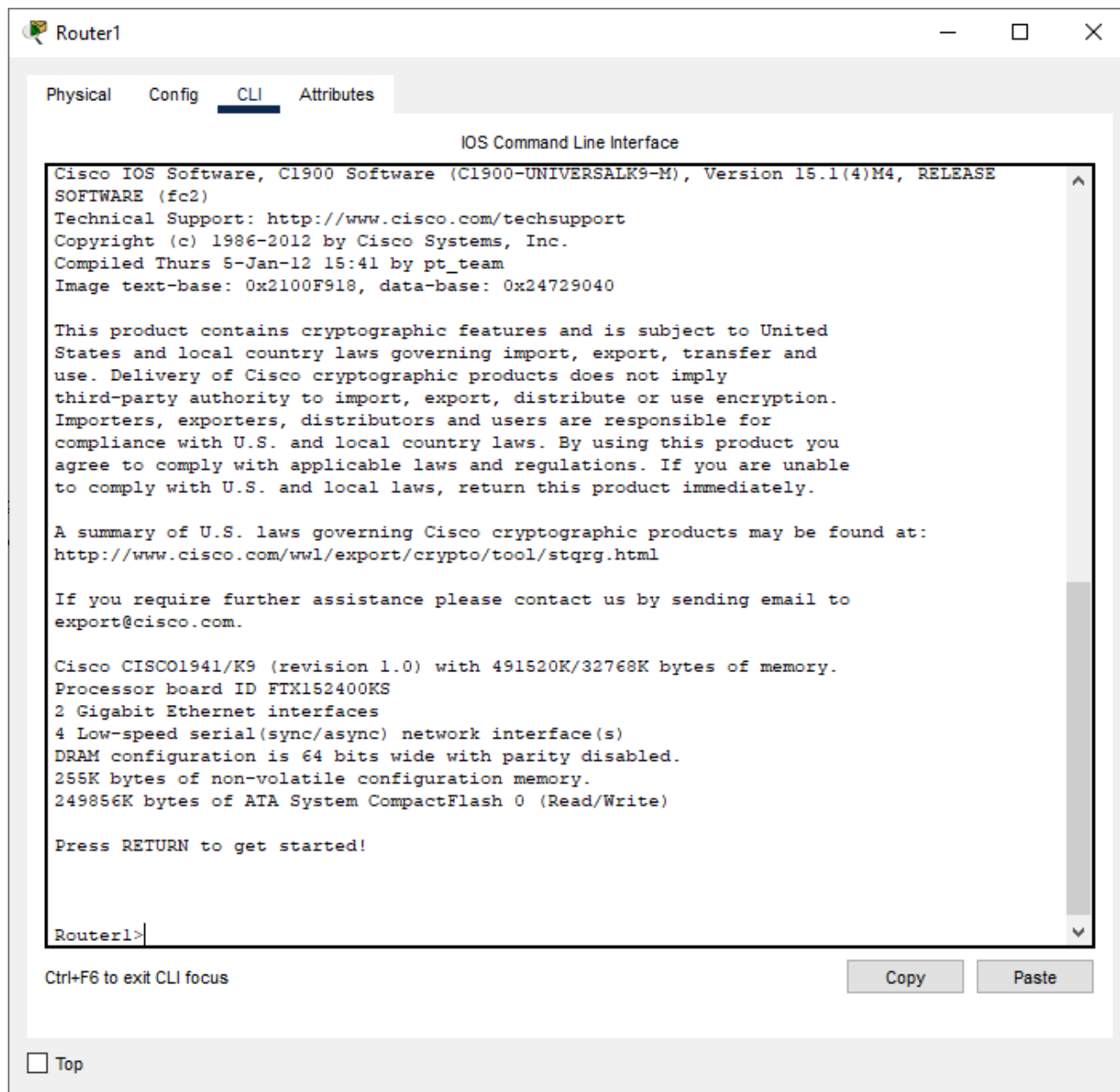
Estando los equipos finales con su configuración IP correcta, ¿deberían poder conectarse entre sí? Realice las siguientes comprobaciones

- Utilizando la interfaz de mandatos de un PC compruebe, haciendo uso del mandato `ping <dirección_ip_host>` si puede conectarse con otro PC de su subred, y con el router.
- Pruebe la conectividad entre dos equipos de diferente subred (por ejemplo, `PC1-1` y `PC2-2`).

3. Configuración TCP/IP básica de los routers

La configuración TCP/IP de los routers **Router1**, **Router2** y **Router3** se realizará en línea de comandos, (CLI) del IOS de Cisco. De esta forma se simula la configuración de un router real, pues las configuraciones introducidas son las mismas que funcionarían en un router Cisco.

Para acceder a la CLI de cada router, haga click en el mismo y seleccione la tercera pestaña.

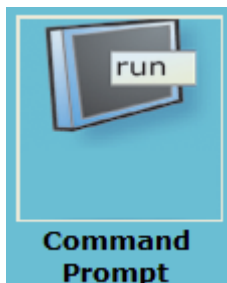


Para cada uno de los routers, se deberá configurar todas sus interfaces utilizadas en la práctica. Por cada interfaz, se deberá configurar su IP, su máscara, e indicar que la interfaz ha de permanecer habilitada (**no shutdown**). A continuación se indican los mandatos que se deben utilizar de manera breve, encontrará más información acerca de los mandatos IOS a utilizar en la [guía de uso del simulador](#) y la [hoja de referencia rápida](#) que acompaña este enunciado.

Descarte el proceso de configuración automático si el router se lo sugiere. Ingrese en el modo de ejecución privilegiado y, a continuación en el modo de configuración, con los mandatos **enable** y **configure terminal**, respectivamente. A configuración, ingrese en el modo de configuración de la interfaz seleccionada utilizando **interface <tipo> <numeración>**, donde el tipo es **FastEthernet**, **GigabitEthernet** o **Serial**, y la numeración serán 2 ó 3 números separados por barras. Pasará al modo de configuración de interfaz, en el que se muestra el prompt

como `(config-if)#` En este modo, ingrese la configuración IP con el mandato `ip address <ip> <mascara>` e indique que la interfaz permanezca activa con `no shutdown`.

Para comprobar el funcionamiento de la interfaz recién configurada, salga al modo de ejecución privilegiado (`end` para salir directamente al modo de ejecución privilegiado), y pruebe a hacer un ping a otro equipo ya configurado **de la misma red**. También puede realizar pings desde los equipos a través de su herramienta *Command Prompt* en la pestaña *Desktop*:



- Obtenga la lista de direcciones IP de los routers `Router1`, `Router2` y `Router3` utilizando el comando `show ip interface brief` en el *modo de ejecución privilegiado*
 - ¿Aparece en dicho listado breve la máscara utilizada? ¿cómo puede comprobar la máscara configurada en cada interfaz? Compruebe que las máscaras configuradas coinciden con las requeridas
- Obtenga también las tablas de rutas de los routers `Router1`, `Router2` y `Router3` utilizando el comando `show ip route` en el *modo de ejecución privilegiado*
 - Observe las entradas de la tabla, ¿hay alguna indicación del tipo de cada entrada? ¿podría decir en qué momento se creó cada una de ellas?
- Vuelva a comprobar la conectividad entre un PC y el router de su red

4. Prueba de la conectividad (2)

4.1 Equipos en Redes 4 y 5



- En este punto de la práctica ¿puede acceder a un equipo de la `RED 4` desde otro de la `RED 5`? Utilice el comando `ping` para comprobarlo, y use posteriormente el comando `tracert` para comprobar el camino seguido entre ambos PCs.
- Ingresa en el modo de simulación de Packet Tracer. En este modo, filtrando para que sólo se visualice el protocolo **ICMP**, vuelva a enviar el ping entre un equipo de la `RED 4` y otro de la `RED 5`. Observe las tramas tanto de la petición como de la respuesta, analizando como se encapsula el protocolo ICMP y el valor de los campos `type` y `code`. Puede encontrar explicaciones de estos campos en páginas como <https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml> además de en las transparencias de clase.

4.2 Routers 2 y 3



Realice la misma prueba de conectividad con pings entre los routers **Router2** y **Router3**. Utilice la interfaz CLI del router **Router2** para hacer ping a todas las direcciones IP de **Router3** ¿con cual de ellas conseguirá conectividad?

4.3 Equipos en las Redes 2 y 4

Vamos a realizar la prueba del apartado 4.1, pero entre un equipo de la **RED 2** y un equipo de la **RED 4**.



1. Utilice el mandato **ping**, y luego **tracert** para comprobar hasta dónde llega la comunicación entre los dos equipos escogidos.
2. Teniendo en cuenta la dirección IP destino de dicho **ping** y la tabla de rutas del **Router1** obtenida en el apartado 3, ¿qué hará el router **Router1** con dicho datagrama?

4.4 Funcionamiento de ICMP

El protocolo ICMP se utiliza para notificar errores acerca del nivel de red, en este caso vamos a comprobar su funcionamiento para notificar problemas de encaminamiento.



Ingresa de nuevo en el modo de simulación de Packet Tracer, filtrando de nuevo para que únicamente se visualice el protocolo **ICMP**. Vuelva a generar tráfico entre un equipo de la **RED 2** y un equipo de la **RED 4**, mediante un **ping**. Analice qué ocurre cuando este datagrama llega al último router que responde el **tracert** anterior. ¿Por qué contesta éste router al origen? Investigue el contenido de dicha respuesta en base a los campos **type** y **code** de ICMP. ¿De qué clase es este mensaje ICMP?

Ahora vamos a comprobar el funcionamiento del mecanismo de *tiempo de vida* ó TTL. Para ello vamos a generar un mensaje ICMP con un **TTL=1**, que sólo puede hacerse en el simulador a través del botón *Add Complex PDU* ![Add Complex PDU](images/PDU_complex.png). Haremos click en el equipo origen y se abrirá el siguiente diálogo donde tendremos que establecer la IP destino, el valor de TTL a 1, un número de secuencia cualquiera y un número de segundos para el intervalo, aunque mandemos sólo un datagrama. Se pulsa el botón de *Create PDU* y se va avanzando la simulación paso a paso.

Create Complex PDU

Source Settings

Source Device: Router1
Outgoing Port:

Auto Select Port

PDU Settings

Select Application: PING
Destination IP Address:
TTL: 32
TOS: 0
Sequence Number:
Size: 0

Simulation Settings

☒ One Shot Time: Seconds
☐ Periodic Interval: Seconds

Create PDU



¿Decrementa el switch el valor de TTL? ¿Qué mensaje se genera en el dispositivo que lo decrementa a 0 y, por lo tanto, no puede seguir encaminando el datagrama? Utilice el campo `type` del mensaje y la tabla de códigos indicada anteriormente.

NOTA: El simulador imprime el valor del campo `type` en hexadecimal, lo que se sabe porque muestra el valor precedido de `0x`.

4.5 Routers no directamente conectados



Realice la misma prueba de conectividad con pings entre los routers que no están directamente conectados. Utilice la interfaz CLI de un router para hacer ping a todas las direcciones IP del otro router, ¿consigue conectividad con alguna de ellas?

- Teniendo en cuenta la IP destino y las tablas de rutas de todos los routers, ¿cuál cree usted que descarta el paquete? Utilice el comando `tracert` (equivalente a `tracert`, pero en un router) para comprobarlo.

5. Configuración de rutas indirectas

Configure en los routers **Router1**, **Router2** y **Router3** rutas indirectas estáticas a las subredes de la universidad que no estén conectadas directamente. Se pretenden crear **todas** las entradas indirectas a las subredes internas, una por cada subred no conectada directamente. **No cree rutas por omisión de momento.**



¿Qué dirección IP ha de utilizar como *siguiente salto* en cada caso?

Realizado este paso debería tener conectividad entre todos los PCs y routers internos de la universidad.



1. Realice todas las comprobaciones que no funcionaron en el apartado anterior. Puede ir comprobando cada ruta con pings hacia la interfaz del siguiente salto, pero tenga en cuenta que un ping utiliza una ruta en un sentido, y otra ruta en el otro para la respuesta (se necesita una ruta para volver).
2. Obtenga nuevamente las tablas de rutas de los routers **Router1**, **Router2** y **Router3**

6. Salida hacia internet



1. Desde un equipo de la **RED 3** compruebe la conectividad con el servidor externo **www.marca.es**, *Desktop > Web Browser*. ¿Alcanza su objetivo? Utilice de nuevo la herramienta **tracert** o **traceroute** para averiguar dónde está el error o envíe pings incrementalmente.

Para direccionar equipos en redes cuyas IP se desconocen *a priori*, como Internet, se utilizan rutas por omisión en las que la máscara y la dirección IP destino son **0.0.0.0**. Establezca rutas por omisión en los routers **Router1**, **Router2** y **Router3** para que direccionen todo el tráfico no interno hacia el proveedor ISP.

- Tenga en cuenta que al crear una ruta, se indica como destino el *siguiente salto*, que no tiene que coincidir con la dirección pública del ISP.



Compruebe nuevamente la conectividad con el servidor externo **www.marca.es**.
¿Alcanza su objetivo?

6.1 Funcionamiento de NAT

Dado que la red de la universidad utiliza direccionamiento privado, y la parte de Internet está configurada como direccionamiento público, el router **Router1**, que se encuentra entre la parte pública y privada, tiene que realizar traducciones de direcciones NAT, utilizando su única dirección IP pública como origen de todos los paquetes que salen, combinándolo con un puerto de TCP ó UDP libre.

Para ello, el router **Router1** ya está configurado para realizar tareas de NAT (en concreto, NAT) y mantiene una tabla de traducciones NAT.



Desde un equipo de la **RED 5** acceda mediante HTTP (petición web con el navegador de un PC) a **www.marca.es** y localice en la tabla de traducciones NAT de **Router1** (mandato **show ip nat translations** ejecutado en modo privilegiado, no en configuración) todas las traducciones asociadas al PC que utilizó.

- De entre las entradas encontradas, ¿cómo se puede saber a qué servicio se accedió con cada una de ellas? ¿ve evidencias de conexiones a servidores HTTP (puerto remoto **TCP 80**) y DNS (puerto remoto **UDP 53**)?

Ingrese en el modo de simulación de Packet Tracer. En este modo, filtrando para que sólo se visualice el protocolo **HTTP**, genere una petición Web a **www.marca.es** desde un equipo de la **RED 5**.



Capture el contenido del paquete que transporta *la petición HTTP* antes y después de atravesar el router **Router1**. Analice dicho contenido en busca de las direcciones IP antes y después de atravesar el router en busca de cambios. Realice lo mismo con la respuesta HTTP.

Puede utilizar un equipo nuevo de la **RED 5** (con la caché DNS vacía) para comprobar también cómo cambian las direcciones de la petición DNS previa a la solicitud HTTP.

6.2 NAT y servidores internos

La universidad ha decidido poner un servidor Web en sus propias instalaciones, para lo cual ha elegido la **RED 5**.

Cree un servidor y conéctelos a **Switch5**, asignándoles una configuración IP de la **RED 5**. En la pestaña *Services* active el servicio HTTP, modificando el fichero **index.html** para comprobar que accede a su propio servidor. Compruebe el servicio utilizando un PC de la universidad (acceda por IP, no por nombre simbólico).

Si queremos acceder desde el exterior de la universidad será necesario asociar los puertos bien conocidos de ambos servicios en la única dirección IP pública que disponemos, a las máquinas en las que están ejecutándose dichos servicios. Esto lo realizaremos con el siguiente mandato en **Router1**:

```
ip nat inside source static (tcp | udp) <IP privada> <puerto privado>
                                <IP publica> <puerto publico>
```

NOTA: es una única línea pero se representa en 2 porque no cabría en una única línea. Se ha de elegir entre tcp ó udp (los paréntesis ahí y el **|** indican *elección*)



Realice la asociación de los puertos TCP 80 (HTTP) con el mismo puerto 80 en el servidor recién creado. Si ahora quisiéramos ofrecer acceso a los servicios de SSH (puerto 22 de TCP) de todos los routers internos desde el exterior, ¿podríamos utilizar los puertos bien conocidos para asignarlos de forma estática?

Para que el servidor interno pueda ser accedido mediante un nombre simbólico (e.g. **www.miservidor.es**), deberemos añadir una entrada en el servidor DNS de Internet. Para ello, haga click

en el servidor y vaya a *Services > DNS*. Ahí introduzca una nueva entrada especificando el nombre simbólico (e.g. `www.miservidor.es`) y la dirección IP correspondiente, es decir la traducción DNS correspondiente.



- ¿Que dirección IP debe especificar en la traducción DNS?

Pruebe la traducción DNS haciendo una petición desde el navegador web de un equipo de Internet (e.g. PC-Casa) y verifique que puede acceder al servidor interno.

Trate ahora de hacer un ping desde el mismo equipo de Internet al servidor interno, usando su dirección simbólica (i.e. `ping www.miservidor.es`).



- ¿Qué sucede? ¿Llega el ping al servidor interno? ¿Por qué se produce esto?

7. Simplificación de tablas de rutas

Acceda de nuevo a la tabla de rutas de los tres routers. ¿Es redundante alguna de las entradas?



Imprima las tablas de rutas de los 3 routers y busque entradas que realizan lo mismo que otras más genéricas, con el mismo *siguiente salto*.

Realice las modificaciones necesarias en los routers, eliminando las entradas que sobren.

Compruebe la conectividad entre todas las redes de la organización y hacia Internet. Se debería seguir pudiendo conectar todos los equipos entre ellos y hacia Internet. Si alguna prueba falla, realice un `tracert` para determinar cual es el punto de fallo y analice las tablas de rutas del router o routers involucrados.

Tenga en cuenta que, para que una petición ICMP funcione, tenemos que tener una ruta del origen al destino, y una ruta inversa.



Imprima la tabla de rutas de los 3 routers después de la simplificación.

Nota: para eliminar una ruta basta con configurar exactamente la ruta a borrar precedida de un `no`. Puede copiar la ruta introducida mostrando la configuración completa del router con el comando `show running-config` que tiene que introducirse en el *modo de ejecución privilegiado* (prompt con `#`)