FUNDAMENTOS DE REDES DE COMPUTADORAS

Guiones de prácticas de laboratorio

UVa

Universidad de Valladolid

Autores: Jesús M. Vegas Hernández, Juan A. Muñoz Cristóbal, Javier Isaac Ramos López, Blas Torregrosa García, Irene Lavín Perrino

Departamento de Informática

Universidad de Valladolid

Julio 2024

Versión 2.0

Con el apoyo de VirtUva

Proyecto de Innovación Docente 2023-24

PRESENTACIÓN

Los presentes guiones de trabajo corresponden con las prácticas de laboratorio de la asignatura Fundamentos de Redes de Computadoras, del Grado en Ingeniería Informática de la UVa. Ésta es una asignatura introductoria a las redes, en donde el estudiantado aprende las nociones básicas de redes usando un analizador de protocolos (wireshark) y un simulador de redes (Cisco Packet Tracer). Las prácticas se implementan como cuestionarios de Moodle, en los que van apareciendo preguntas aleatorias de bancos de preguntas, de forma que las preguntas que aparezcan a distintos estudiantes sean similares, pero no iguales. Las prácticas se dividen en dos bloques, un primer bloque en el que se usa wireshark, y uno segundo en el que se utiliza Packet Tracer. Se recomienda que al finalizar cada bloque haya un ejercicio entregable, o pequeño proyecto, en el que cada estudiante deba trabajar los conocimientos de dicho bloque y entregar un informe, captura y/o red.

El motivo de la redacción de este documento es el de ofrecer un material de apoyo al alumnado de la asignatura de Fundamentos de Redes de Computadoras, así como que pueda servir se ayuda en otras asignaturas de la UVa o de otras organizaciones educativas.

Tabla de contenido

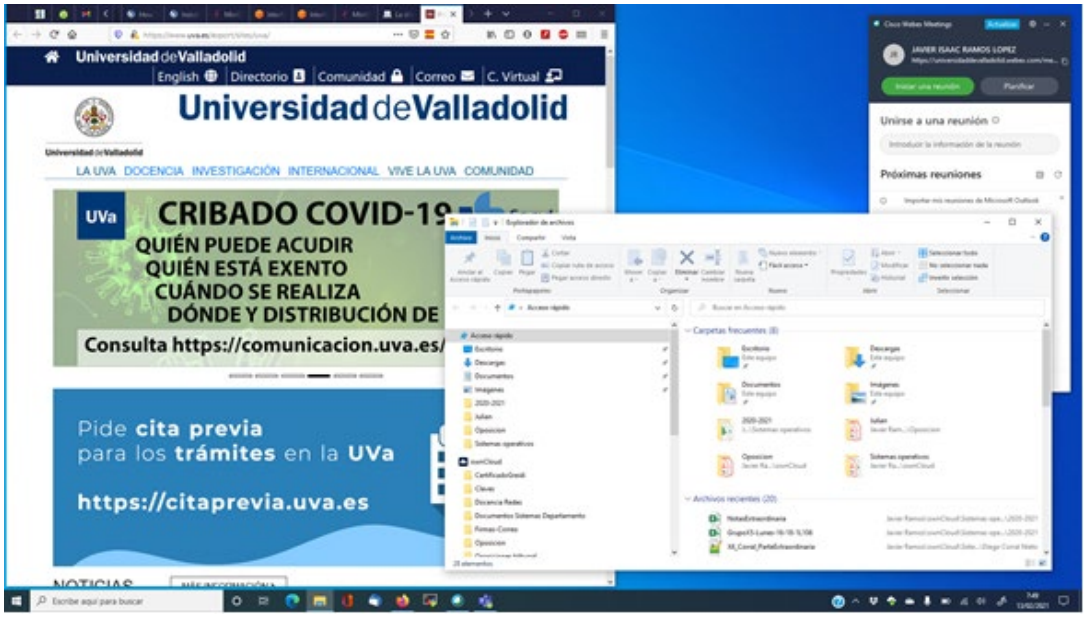
1. Breve introducción al Shell de **UNIX**

1.1 Interfaz de usuario

Podemos denominar interfaz de usuario al medio con que el usuario puede comunicarse con una máquina, equipo, computadora o dispositivo. Es un concepto general, que aplica a todos los sistemas informáticos que requieran de interacción humana. En el caso de ordenadores y dispositivos de red, podemos distinguir entre dos tipos de interfaces de usuario: Entorno de escritorio o interfaz gráfica, y entorno de terminal o consola.

1.1.1 Entorno de Escritorio

Un entorno de escritorio, también llamado entorno gráfico, o interfaz gráfica de usuario (GUI, de las siglas en inglés), es un conjunto de software para ofrecer al usuario de una computadora una interacción amigable y cómoda. Es una implementación de una interfaz gráfica que ofrece una serie de herramientas para que el usuario interaccione con aplicaciones de una forma más cómoda y eficiente. En estos entornos disponer de una tarjeta gráfica mejora la eficiencia del sistema



Pros:

- Obtendrá una experiencia informática completa con poca configuración necesaria, sin necesidad de aprendizaje.

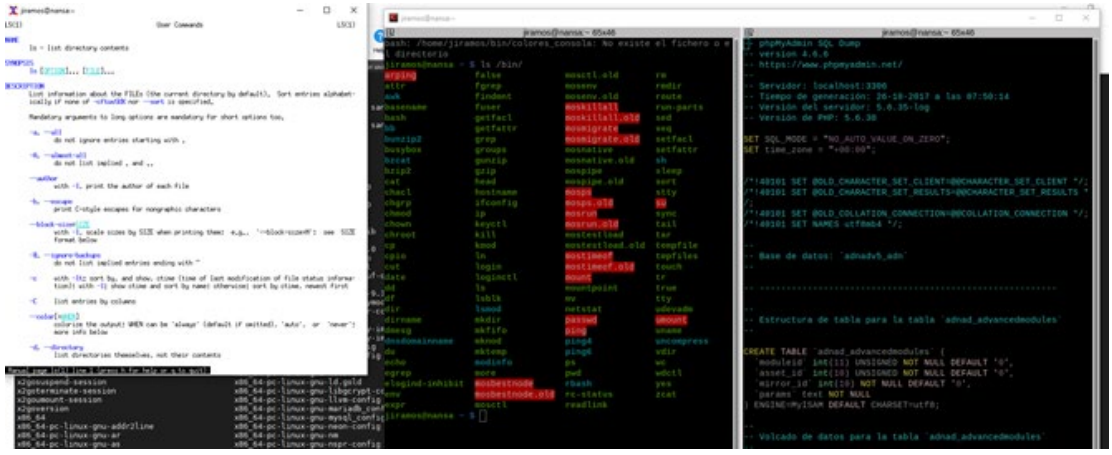
- Gran cantidad de widgets que ayudan a mejorar la productividad.
- Una curva de aprendizaje muy baja

Contras:

- Lentitud y sobrecarga del sistema.
- Gran cantidad de programas preinstalados que no se usan.
- La personalización a veces no es sencilla y afecta al rendimiento.

1.1.2 Entorno de Terminal o Consola

Se denomina terminal o consola (hardware) a un dispositivo electrónico o electromecánico que se utiliza para interactuar con un computador. Un terminal puede definirse como cada uno de los ordenadores conectados a la red. También recibe el nombre de nodo o estación de trabajo. En el inicio de la informática, ésta era la forma de trabajo habitual. Los terminales no tenían capacidad gráfica, y se trabajaba siempre utilizando comandos textuales.



Un avance relacionado con los terminales fueron los sistemas de tiempo compartido, que se desarrollaron con la capacidad de soportar a múltiples usuarios conectados a la misma máquina, cada uno de ellos con su propio terminal.

Debido a la tradición histórica, las interfaces de usuario que usan un modo textual, sin gráficos, se han seguido llamando interfaces de terminal o de consola. También se les denomina interfaz de línea de comandos (CLI, de las siglas en inglés).

La administración de equipos y su sistema operativo ya sea de forma local o remoto gracias a los terminales resulta más eficaz la mayoría de las veces comparado con el uso de entornos gráficos.

Pros:

- Menos uso de memoria y CPU que los entornos de escritorio
- No requiere gran potencia gráfica
- Altamente configurable para una máxima comodidad.
- Están centrados en el teclado, se realiza un trabajo más eficiente.
- La mayoría de los sistemas se pueden gestionar en entornos de terminal:
    - Windows Core (PowerShell)
    - Unix Shell, Bash, Csh, Ksh etc.
    - Gestión de Swithes, Router, Firewall
    - Cabinas de almacenamiento
    - Gestión de dispositivos de red, etc.

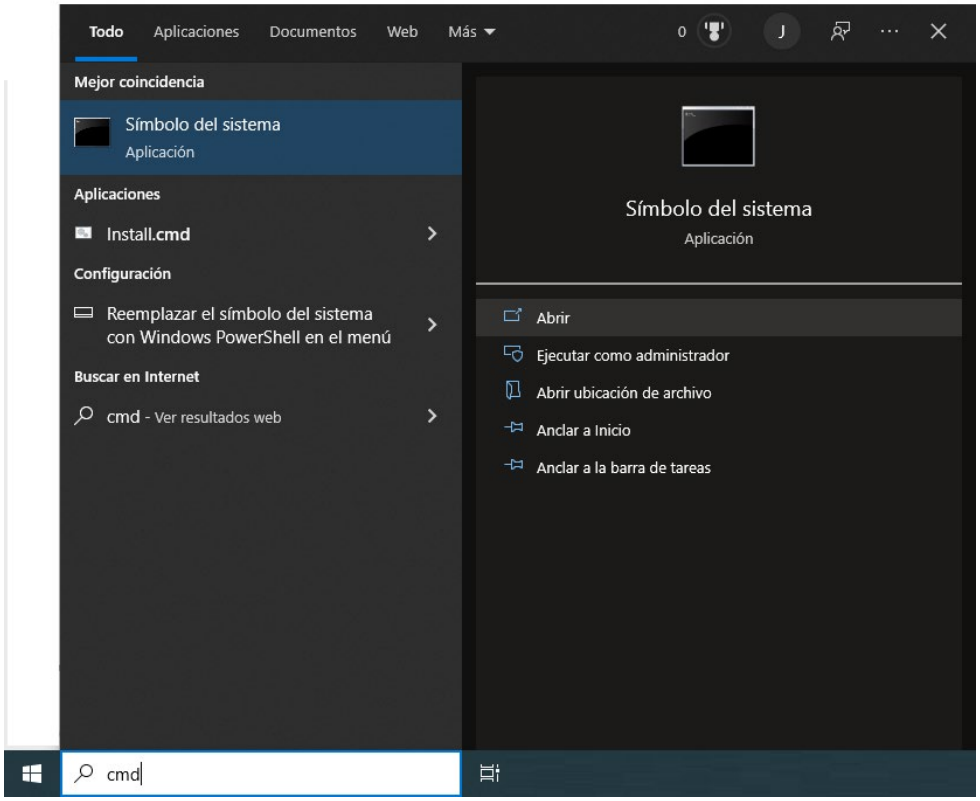
Contras:

- No es tan fácil de usar como lo es un entorno gráfico
- No es tan atractivo visualmente como lo es un entorno de escritorio
- Curva de aprendizaje pesada

> Aquí se incluyen dos preguntas aleatorias de sendos bancos de preguntas sobre escritorios gráficos y terminales de consola.

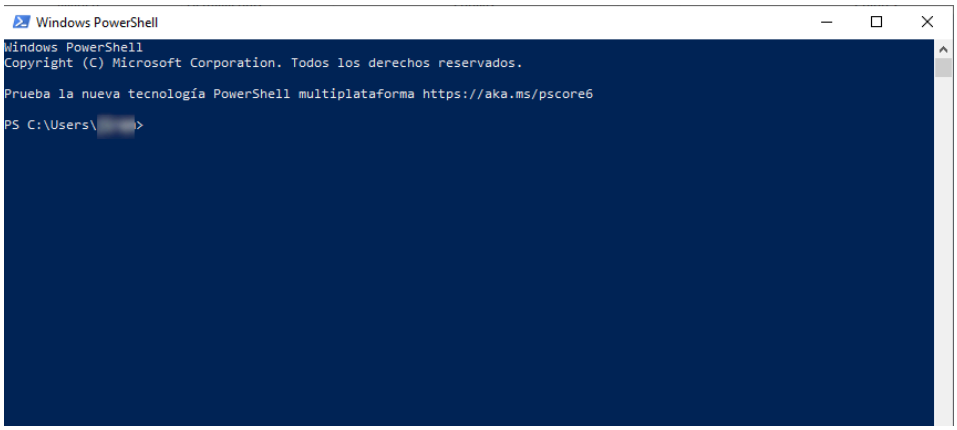
1.2 Entornos de terminales en Windows

En Windows disponemos de dos terminales de tipo CLI (*command-line interface*) que podremos lanzar usando el buscador integrado en la barra inferior de Windows. Estos dos son:



- **Cmd**, los comandos disponibles en este sistema son mucho más reducidos que en el nuevo entorno de Microsoft PowerShell. Cmd se mantiene por compatibilidad con sistemas anteriores a los actuales.

- **PowerShell** es una solución de automatización de tareas multiplataforma formada por un shell de línea de comandos, un lenguaje de scripting y un marco de administración de configuración. También está disponible en Linux y MacOS.

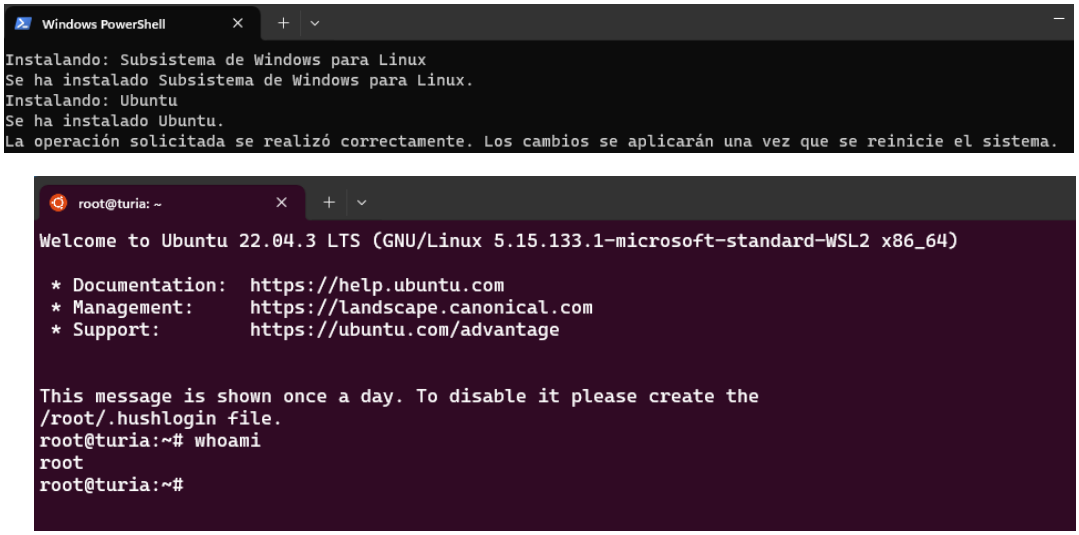


- **Subsistema Linux para Windows.** WSL (Windows Subsystem for Linux) es una característica de Windows que permite ejecutar un entorno Linux directamente en un sistema Windows sin necesidad de una máquina virtual.

  Para activar el Subsistema Linux para Windows (WSL) habría que seguir estos pasos (**NO hay que seguirlos en la práctica**):

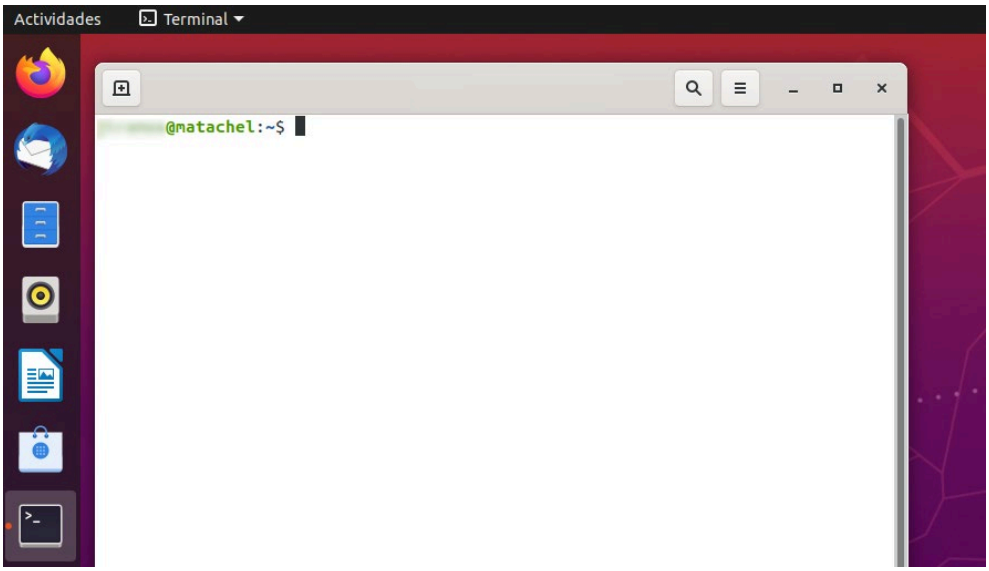
1. Abrir el "Panel de control" de Windows.
2. Ir a la sección "Programas" o "Programas y características".
3. Hacer clic en "Activar o desactivar las características de Windows".
4. Buscar "Subsistema de Windows para Linux" en la lista y marcar la casilla junto a él.
5. Hacer clic en "Aceptar" y seguir las instrucciones para reiniciar el sistema si es necesario.

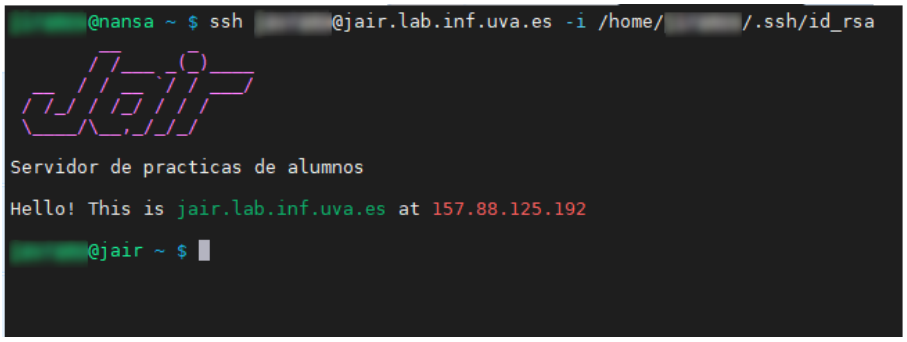
Después de reiniciar, se puede instalar una distribución de Linux desde la Microsoft Store o utilizando el comando `wsl --install` en PowerShell. Una vez instalado, ya se podría utilizar el Subsistema Linux para Windows.



1.3 Entornos de terminales Linux y MacOS

En estos dos sistemas operativos disponemos de terminales que nos proporcionan un lenguaje de scripting y automatización basados en Shell. Disponemos de varios tipos de terminales, pero el más extendido es el basado en Bash scripting.





1.4 Comandos básicos en los terminales

- Listar ficheros y directorios. Para ello tenemos dos comandos: **dir** que funciona en la consola cmd y en PowerShell y **ls** que funciona solo en PowerShell, MacOS y en linux.
- Copiar un archivo de un origen a un destino. El comando para PowerShell y Cmd sería:

  copy <archivo_origen> <archivo_destino>

  En PowerShell, MacOS y en Linux sería

  cp <archivo_origen> <archivo_destino>
- Eliminar un archivo, el comando para cmd y PowerShell es:

  del <nombre_de_archivo>

  En PowerShell, MacOS y en Linux sería:

  rm <nombre_de_archivo>
- Mover un archivo de una ubicación a otra, también se usa para renombrar.

En cmd y PoweShell sería:

move <archivo_origen> <archivo_destino>

En Linux, MacOS y PowerShel sería:

mv <archivo_origen> <archivo_destino>

- Crear un directorio o carpeta en todos los sistemas es un comando igual:

  mkdir <nombre_carpeta>

- Eliminar una carpeta o directorio, en todos los sistemas es el mismo comando:

  rmdir <nombre_carpeta>

> Aquí se incluyen tres preguntas aleatorias de sendos bancos de preguntas sobre comandos básicos de terminales.

1.5 Comandos de conexión a equipos remotos

Existen muchos protocolos que permiten la conexión entre equipos remotos. Nosotros nos centraremos en el protocolo SSH que nos permite conectarnos de forma segura de un servidor a otro y abrir un terminal.

SSH es un protocolo que garantiza que tanto el cliente como el servidor remoto intercambien informaciones de manera segura y dinámica. El proceso es capaz de encriptar los archivos enviados al directorio del servidor, garantizando que las alteraciones y el envío de datos sean realizados de la mejor forma.

Para conectarse a un equipo remoto debemos conocer, o bien su dirección IP, o bien su FQDN (*fully qualified domain name*), también llamado nombre DNS. Los nombres de DNS están compuestos por un nombre de host y un dominio separados por un punto: <hostname>.<dominio>. El dominio identifica una subárea de una red (normalmente Internet), y a su vez está compuesto por una serie de etiquetas separadas por puntos. Por ejemplo, en nuestro caso tenemos un servidor que se llama ***jair*** que está en el dominio ***lab.inf.uva.es***, que sería nuestro domino. Por lo tanto, el nombre DNS de la máquina será **jair.lab.inf.uva.es**.

Otro dato que debemos conocer es el nombre de usuario y contraseña para poder acceder al equipo, sólo los usuarios autenticados y permitidos podrán acceder a la máquina por el protocolo SSH. La Escuela de Ingeniería Informática de Valladolid proporciona estos datos a todos los alumnos para el acceso a las máquinas de la escuela, como es el caso de jair.

1.5.1 Conexión remota

Para conectarnos a la máquina de forma remota disponemos de un comando que es ***ssh***, este comando es igual para todos los tipos de terminales que estamos tratando. Su formato es:

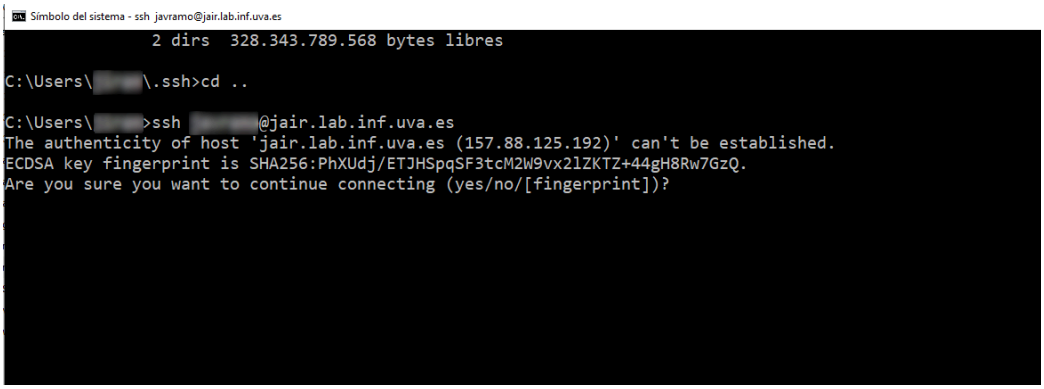
ssh <nombre_de_usuario>**@**<nombre_DNS_de_equipo>

o bien

ssh <nombre_DNS_de_equipo> **–l** <nombre_de_usuario>

***Nota**: Los corchetes no hay que escribirlos.*

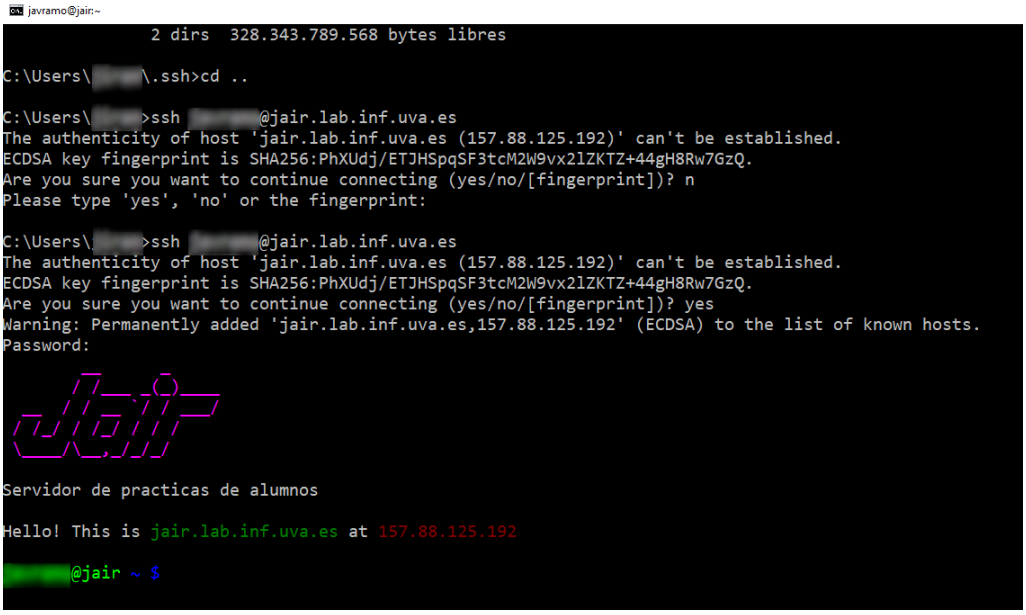
Posteriormente, si es la primera vez que nos conectamos a esa máquina nos preguntará si queremos admitir la huella digital o fingerprint que debemos contestar que sí.



El fingerprint es una huella digital de clave pública, en la criptografía de clave pública, es una secuencia corta de bytes utilizada para identificar una clave pública más larga. Las huellas digitales se crean al aplicar una función de cifrado hash a una clave pública. En nuestro caso nos sirve para identificar al servidor al que nos conectamos para evitar, por ejemplo, ataque de tipo Man In The Middle (o ataque de Intermediario).

Por último, nos pedirá la clave para ese usuario. Por seguridad, al escribir la contraseña no se muestran los caracteres que se van escribiendo. Esto puede confundir un poco al principio y puede parecer que no funciona el teclado, pero sí que funciona. Debemos escribir la contraseña y pulsar la tecla de retorno de carro.

Una vez autenticado nos abrirá un terminal en el equipo remoto desde ese momento podremos ejecutar comandos de SHELL en la máquina remota. Podemos distinguir que estamos conectados a una máquina remota por el prompt. Por ejemplo, en la siguiente figura el prompt nos muestra que estamos conectados en jair.



Si estamos conectados remotamente a un equipo mediante ssh y queremos desconectarnos y volver a nuestro PC local, el comando para hacerlo es: **exit**

1.5.2 Copia de archivos entre equipos remotos.

El protocolo ***ssh*** permite copiar archivos desde la máquina local a la remota y viceversa. Para ello disponemos de un comando que es ***scp***, este comando existe en todos los terminales de los sistemas operativos. Su formato es el siguiente:

scp <origen> <destino>

Siendo <origen> un archivo local o remoto. Si es local se debe especificar el nombre del archivo y el camino (path) para llegar a él. Y si es remoto el formato es el siguiente:

<nombre_de_usuario>**@**<nombre_DNS>**:**<nombre de archivo>

Lo único que no se puede hacer es que <origen> y <destino> sean remotos.

Si el nombre del archivo en el destino es igual que en el origen, no hace falta poner el nombre del archivo en el destino.

Por ejemplo, si queremos copiar un archivo de la máquina local que se llama archivo.txt a una remota llamada jair.lab.inf.uva.es **con el mismo nombre de archivo** y con el usuario pepe, el comando sería:

scp archivo.txt pepe@jair.lab.inf.uva.es:

(Nótense los dos puntos del final, y que después de los dos puntos no se pone el nombre de archivo destino, porque es el mismo que el origen)

Y si queremos copiarlo de la máquina remota a la local sería:

scp pepe@jair.lab.inf.uva.es:archivo.txt C:\archivo.txt

Es importante no olvidar los **:** al final del nombre de la máquina remota.

Aquí se incluyen tres preguntas aleatorias de sendos bancos de preguntas sobre comandos de gestión de ficheros en servidores remotos.

1.6 Comandos básicos para Redes

Los comandos básicos para la gestión de la red en los sistemas son los siguientes:

- **Conocer la dirección IP del equipo**. La dirección IP, también comúnmente llamada sólo IP (por sus siglas en inglés, Internet Protocol, o Protocolo de Internet) es un código numérico que identifica una interfaz, dispositivo o red, que usa el protocolo IP. IP es un conjunto de reglas utilizadas para establecer comunicaciones a través de internet. Por lo tanto, cada dirección IP identifica una red o dispositivo en internet. Es importante saber cómo obtener la dirección ip del dispositivo con el que estamos trabajando. Para ello podemos hacerlo entrando en web como https://www.cual-es-mi-ip.net/ o usar un comando, que es lo recomendable.
  El comando, en cmd y en PoweShell es ***ipconfig***, mientras que en Linux y MacOS es ***ifconfig***

  La salida de este comando es algo distinta en diferentes sistemas operativos, pero la información que aparece es similar. Por ejemplo, la salida del comando en una máquina linux puede ser la siguiente:

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500

 inet 157.88.124.104  netmask 255.255.255.0  broadcast
157.88.124.255
 ether 00:1b:21:9f:66:04  txqueuelen 1000  (Ethernet)
 RX packets 1125644602  bytes 1086861272748 (1012.2 GiB)
 RX errors 0  dropped 7393  overruns 7393  frame 0
 TX packets 308922103  bytes 71465639689 (66.5 GiB)
 TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

  - La primera línea nos muestra el nombre de la interfaz de red (eth1) con el tamaño de mtu (Maximum Transfer Unit). Estudiaremos su significado a lo largo del curso.

- La segunda línea nos muestra la dirección IP que tiene asignada esa interfaz, en este caso 157.88.124.104 la máscara de red, que estudiaremos su significado a lo largo del curso, 255.255.255.0 así como la dirección de broadcast de la red 157.88.124.255
- La tercera línea nos muestra la dirección MAC que está asociada al hardware en este caso 00:1b:21:9f:66:04. La dirección MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo.
- Las siguientes dos líneas son contadores de paquetes recibidos y paquetes recibidos con error.
- Y las dos últimas son contadores de paquetes transmitidos y paquetes transmitidos con error.

- **Conocer la puerta de enlace o gateway**. Para ello podemos consultar la tabla de rutas. Veremos más adelante qué es una tabla de rutas, pero a nivel básico es un listado de los distintos destinos a los que el dispositivo puede enviar tráfico, y por dónde debe enviar el tráfico para alcanzar cada destino. El tráfico hacia un destino distinto de la propia red en la que está el dispositivo se envía hacia un gateway (un router que enlaza dos redes). Para obtener la tabla de rutas en todos los sistemas se usa el mismo comando, ***route***, la diferencia es que en Linux y MacOS muestra la ruta sin tener que poner ningún parámetro al comando, por el contra, en PowerShell y Cmd hay que poner ***route print***
  La salida del comando route -n en una máquina Linux es:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric
Ref    Use Iface
0.0.0.0         10.xxx.xxx.xxx    0.0.0.0         UG    100    0
    0 ens18
10.xxx.0.0      0.0.0.0         255.255.0.0     U     0      0
  0 ens18
```

La salida nos muestra en la primera línea, segunda columna, la IP 10.xxx.xxx.xxx[1] que es el router (o gateway) por defecto. Esto lo podemos saber por la primera columna que pone la ip 0.0.0.0 (0.0.0.0 significa "cualquier dirección IP") y por la columna de los Flags que pone UG. El router por defecto será el equipo al que mandaremos todo el

[1] Se oculta parte de la información por cuestiones de privacidad y seguridad.

tráfico que sea como destino cualquier IP que no sea de mi red. En este caso "mi red" la indica la IP de la segunda línea 10.xxx.0.0

- **Comando de manejo del DNS** en todos los sistemas es el mismo ***nslookup***

Con este comando podremos saber qué IP corresponde con un nombre de internet. Así pues, si ejecutamos el comando ***nslookup www.uva.es*** obtendremos de respuesta:

```
Server:         157.88.124.249
 Address:        157.88.124.249#53
 Non-authoritative answer:
 Name:   www.uva.es
 Address: 157.88.25.8
```

- La primera línea nos indica qué servidor DNS nos contesta, la segunda nos dice la dirección IP del servidor DNS y el puerto que usa, en este caso el 53 (veremos más adelante lo que es un puerto).
- La siguiente línea es el nombre de internet por el que preguntamos
- y por último la dirección IP que le corresponde a dicho nombre, en este caso 157.88.25.8.

> Aquí se incluyen dos preguntas aleatorias de sendos bancos de preguntas sobre gestión de red en servidores remotos.

> Aquí se incluye una pregunta final de autorreflexión y síntesis sobre la práctica realizada y los conocimientos adquiridos.

2. Introducción a Wireshark

2.1 WireShark

En este ejercicio vamos a presentar una herramienta muy útil para analizar las innumerables comunicaciones en las que interviene nuestro computador, así como los mensajes que las componen y los protocolos que se utilizan para ello.

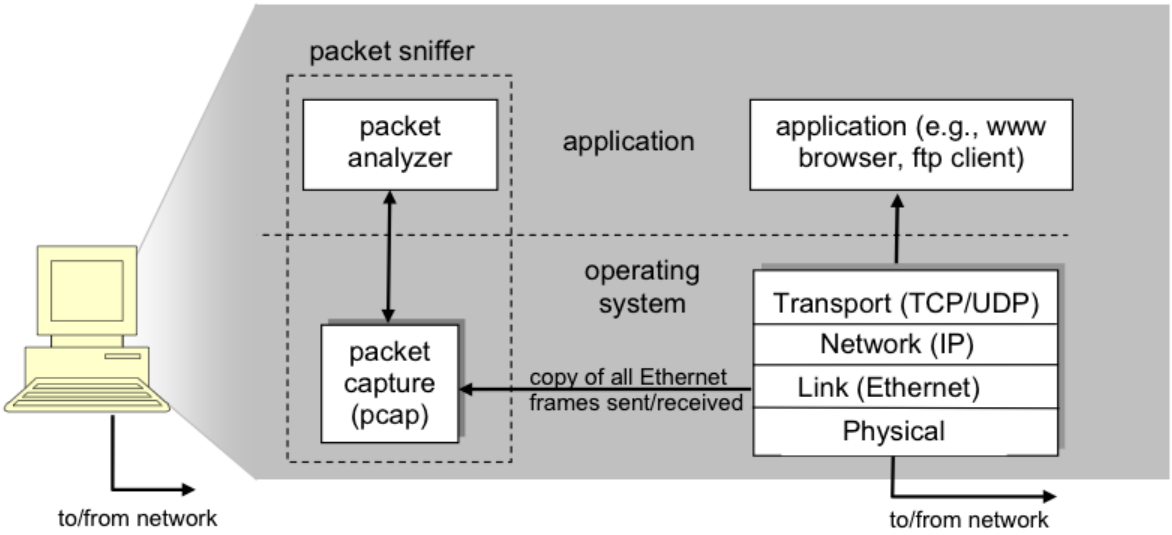
Esta actividad requiere tener acceso a una instalación de Wireshark, existen versiones para todos los sistemas operativos Linux, Windows y MacOS en este link podéis ver las descargas disponibles de la última versión. En los laboratorios disponéis la opción de arrancar un **sistema linux** conectado a la red de los laboratorios que dispone de una versión de Wireshark.

La herramienta Wirehark es una herramienta del tipo "*sniffer*", es decir, un husmeador o cotilla que captura todo paquete que se haya originado o bien tenga por destino la interfaz conectada a la red que se quiere analizar. Un sniffer es una aplicación que retiene una copia de cada paquete que llegue o salga de la interfaz de red elegida, actuando de manera pasiva, sin interferir en el tráfico. Es, por lo tanto, indetectable. Dependiendo de su configuración, cuando una interfaz de red está en **modo promiscuo** incluso puede capturar paquetes que ni siquiera estén asociados a la máquina en la que se ejecuta, pudiendo así interceptar toda la información que pase por el cable y esté a su alcance.

Esta herramienta nos va a permitir observar la red como por un microscopio, filtrando los paquetes por distintos criterios como origen, destino, protocolo, etc. permitiéndonos analizar con minuciosidad cada una de las capas que forman las tramas. Es por ello, un elemento fundamental en el descubrimiento y estudio de las redes. Este tipo de programas que permiten ver en detalle los paquetes, decodificándolos, se llaman analizadores de protocolos.

2.2 Introducción a Wireshark

La Figura 1 muestra la estructura de un "sniffer" de paquetes. Los principales componentes de un sniffer son el capturador de paquetes y el analizador de paquetes. El primero captura los paquetes que son enviados y recibidos por la interfaz, o tarjeta de red. Estos paquetes son decodificados por el analizador, lo que permite la visualización de los mismos y el análisis de las conexiones. El analizador debe ser capaz de interpretar las tramas enviadas por las distintas capas de protocolos implicadas (parte derecha de la figura).

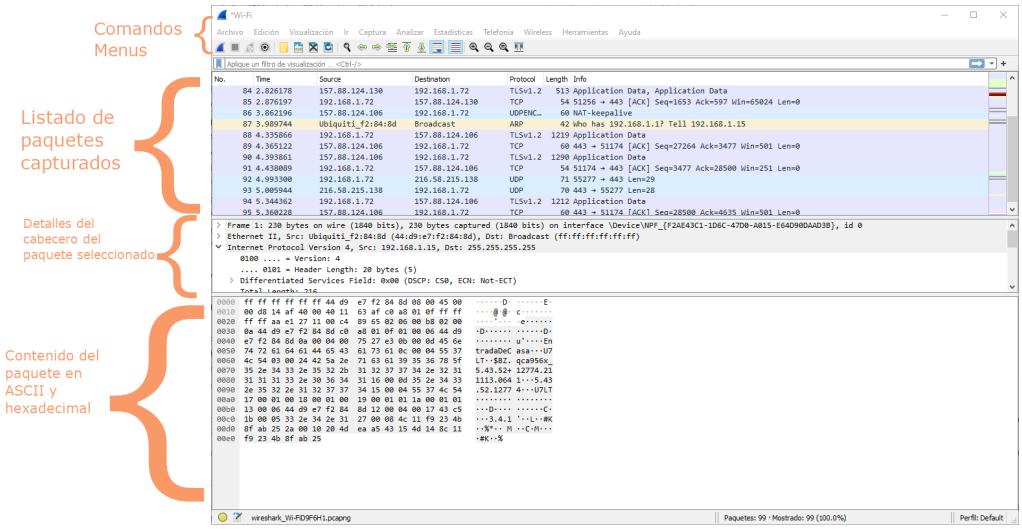


Fuente: James F. Kurose, Keith W. Ross. Computer Networking: A Top-Down Approach. Sixth edition. Pearson. 2013

Nosotros vamos a utilizar Wireshark (https://www.wireshark.org) como sniffer, ya que es una herramienta multiplataforma de código abierto (*open source*) y puede ejecutarse sobre ordenadores Windows, Linux/Unix y Mac. Además, es muy estable, tiene una gran base de usuarios y un soporte documental que incluye una guía de usuario (https://www.wireshark.org/docs/wsug_html_chunked/), páginas de manual (https://www.wireshark.org/docs/man-pages/) y una detallada FAQ (https://www.wireshark.org/faq.html). Además, su funcionalidad es muy completa y permite analizar cientos de protocolos y su interfaz de usuario está bien diseñada. Funciona con ordenadores que utilizan una gran variedad de tecnologías de comunicación como Ethernet, Token-Ring, FDDI, serial (PPP y SLIP), redes inalámbricas 802.11 y conexiones ATM (siempre que el SO sobre el que corre Wireshark lo permita). Es una herramienta que se usa habitualmente en entornos profesionales de ingeniería de redes.

Se puede encontrar más información sobre sniffers en https://en.wikipedia.org/wiki/Packet_analyzer .

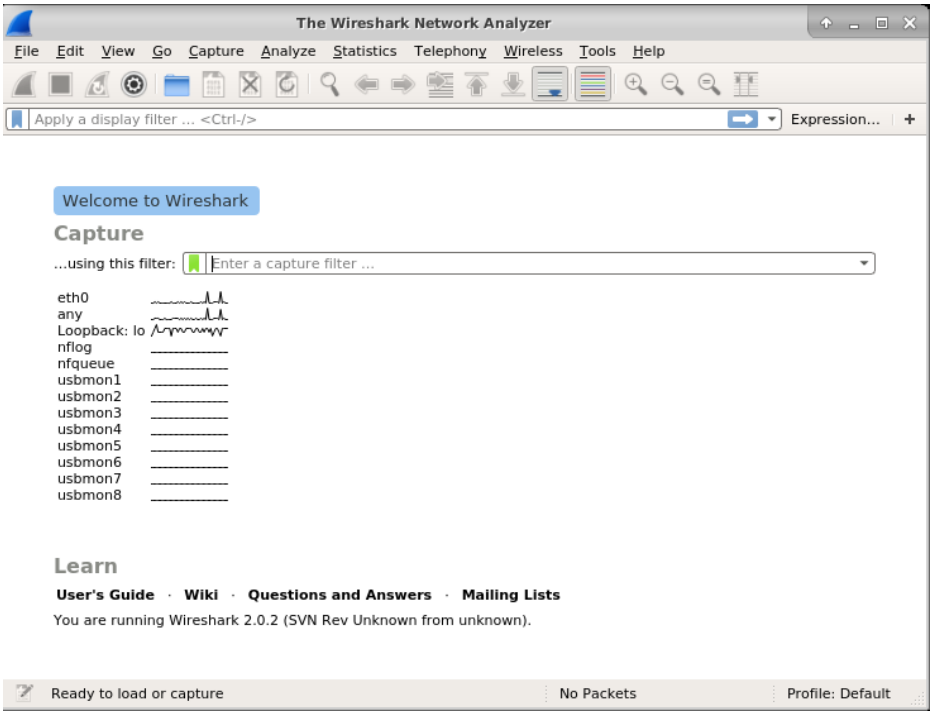
En la Figura 2 se puede observar la interfaz de usuario y las distintas zonas en las que se organiza la información.



2.3 Wireshark Interfaces y Captura

Cuando se ejecuta Wireshark por primera vez, se presenta una ventana con las distintas interfaces detectadas y acceso a documentación, entre otras opciones, tal y como muestra la siguiente figura (los detalles pueden variar entre versiones, SO's y computadores).

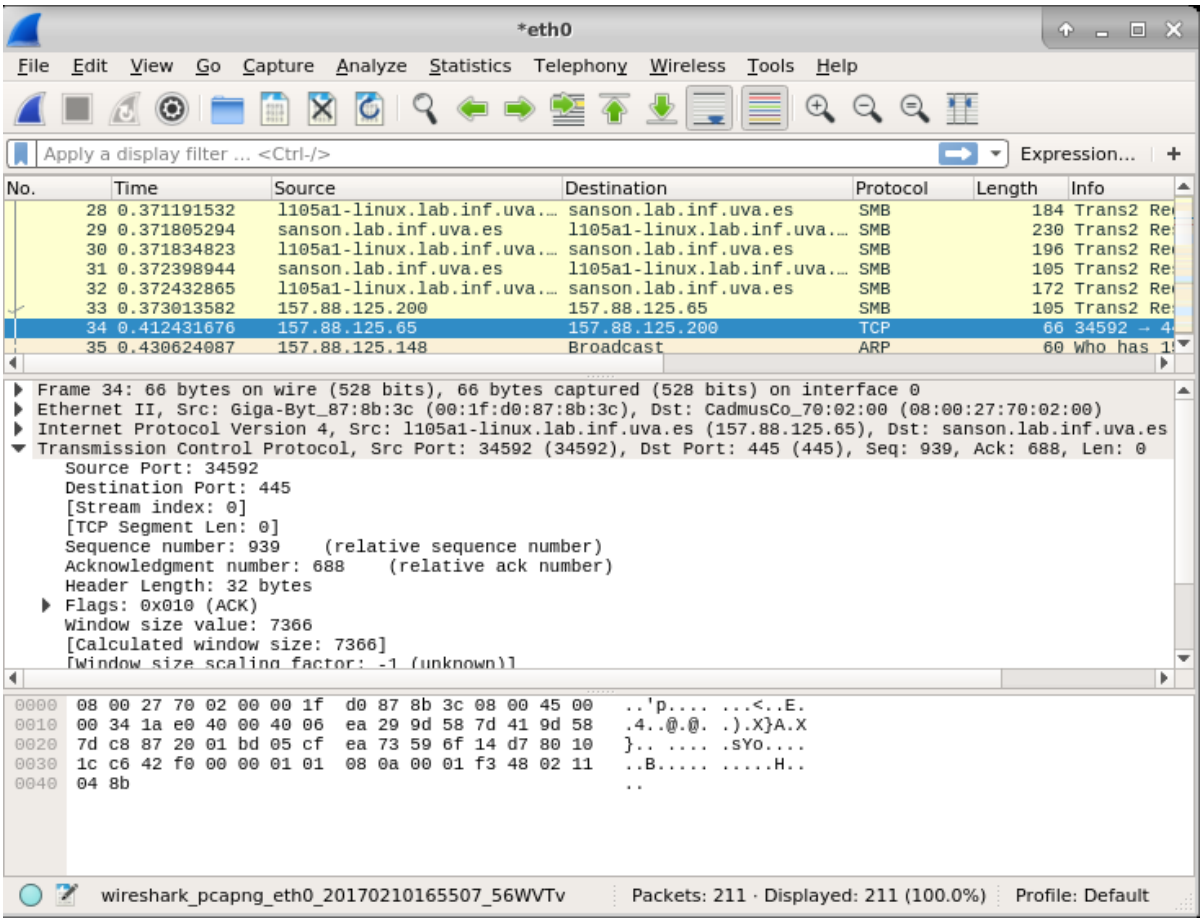
Ha de tener en cuenta que para poder acceder a toda la funcionalidad del programa es necesario tener privilegios de administración en el sistema. De otro modo, por ejemplo, es posible que no pueda acceder al control de las interfaces de red ni activar el modo promiscuo. De todos modos, esto ya ha sido tenido en cuenta en el laboratorio, por lo que no debería tener ningún problema con ello.



Al arrancar la aplicación, ésta busca las interfaces de red disponibles y muestra su actividad con una mini-gráfica. Para iniciar la captura en una interfaz de red de las disponibles, basta con seleccionar la interfaz adecuada y comenzará la captura. Si espera unos segundos, verá en la pequeña gráfica que aparece al lado de cada interfaz qué interfaces tienen tráfico. Haga doble clic en la interfaz que tenga tráfico para iniciar la captura de paquetes en dicha interfaz. Si está conectado por cable será **ethX** o **ensX** o Ethernet X (donde **X** se corresponde con un número, por ejemplo, eth0 o ens18). Si está conectado por wifi, seguramente le pondrá algo como "Wi-Fi", o wlanX.

Una vez que la aplicación está en modo captura se mostrará una pantalla con distintas áreas. En la siguiente figura se muestra (además de los menús y el filtrado) tres paneles distinguibles con:

- el listado de paquetes capturados,
- los detalles del paquete seleccionado, y
- el contenido del mismo.



El panel de listado de paquetes situado en la parte superior de la ventana muestra un resumen de cada paquete capturado. Picando en cada una de las cabeceras de las columnas de la tabla se reordenan los paquetes por el valor en dicha columna.

El panel de detalles del paquete muestra más detalladamente el paquete seleccionado. En el caso de la figura se trata del paquete num. 34, que es un paquete TCP (coloreado en gris oscuro). Fíjese en el tipo de información que se muestra en cada columna:

1. **No.**: Número del paquete en la captura.
2. **Time**: Instante de tiempo de captura del paquete.
3. **Source**: Descripción del origen del paquete. Bien puede indicar la dirección IP (p.e. 157.88.124.251) o el nombre de dominio de la máquina (p.e. dhcp215.dcs.fi.uva.es).
4. **Destination**: Descripción del destino del paquete (IP o nombre de dominio).
5. **Protocol**: El protocolo a que se refiere este paquete.
6. **Lenght**: El tamaño del paquete.
7. **Info**: Descripción del paquete, su cometido, contenido, origen y destino.

El tercer panel, el inferior, muestra los datos reales del paquete en hexadecimal, lo que, aunque en un primer contacto con la herramienta no resultará de especial utilidad, es muy útil cuando se necesita un análisis más profundo de la información de los paquetes.

Las operaciones más habituales a realizar con esta herramienta son la captura de los paquetes y el posterior análisis de los mismos.

- **Captura**: se debe indicar la interfaz de red que realizará la captura. Una vez iniciada la captura de paquetes, wireshark seguirá capturando paquetes mientras no se le indique que pare. La captura puede ser almacenada en un archivo, si se desea, para un posterior análisis.
- **Análisis**: una vez realizada una captura, o bien mientras se procede a la misma, se puede analizar el tipo de paquetes que se envían/reciben/pasan. Para este cometido suele ser conveniente filtrar el tipo de paquetes que se quieren observar, de forma que se centra la atención en los paquetes deseados eliminando las molestias que pueden producir la gran cantidad de paquetes que se suceden.

En la zona de menús, destaca el acceso directo a distintas operaciones. Se puede seleccionar la interfaz sobre la que se realizará la captura (), y controlar la captura tanto para iniciarla (), como para pararla (). También existe un acceso directo a la configuración de la captura (). En la caja de filtrado (Apply a display filter / Aplique un filtro de visualización) se pueden indicar las condiciones que deben cumplir los paquetes mostrados. Estas condiciones pueden llegar a ser muy sofisticadas a fin de seleccionar un tipo concreto de paquete. En este caso se encuentra en blanco, por lo que se muestran todos los paquetes capturados.

Los paquetes capturados pueden ser almacenados en un archivo para su posterior análisis. Todas estas operaciones se pueden hacer en el menú **Archivo**/**File**.

Practique un par de minutos realizando capturas y filtrado de los paquetes. Un ejercicio muy interesante puede ser filtrar los paquetes por origen, por destino o bien por protocolo. También es aconsejable practicar en ordenar los paquetes por distintos valores (columnas) y entender el modo en que se colocan en la tabla.

2.4 Configurar el Programa

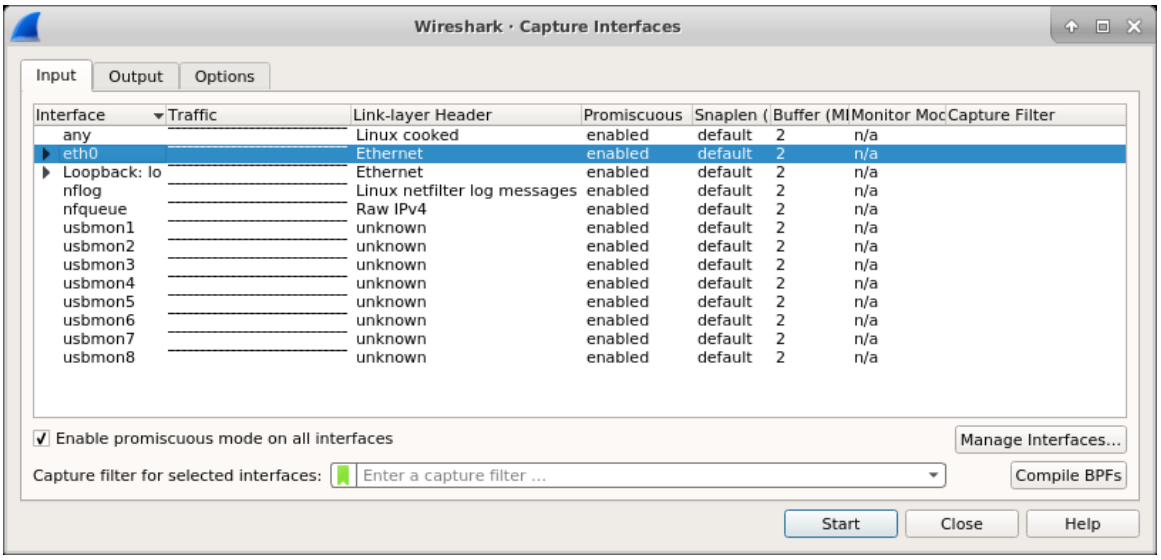
Antes de comenzar a capturar paquetes debemos seleccionar la interfaz de red. Se puede llegar a sorprender por la cantidad de interfaces de red que se pueden encontrar en un computador personal:

- Una interfaz Ethernet cableada.
- Una interfaz WiFi (802.11) inalámbrica.
- Otros dispositivos que pueden considerarse como interfaces de red: Bluetooh, USB, Firewire, etc.
- Una interfaz virtual conocida como "*loopback*", que sirve a los programas del

ordenador para ejecutarse en red aunque el ordenador no esté conectado a ninguna red en concreto (modo *localhost*).

Existen varias formas de seleccionar una de las interfaces. Ahora vamos a hacerlo utilizando la opción de menu **Capture > Options** (Captura > Opciones). La interfaz Ethernet puede tener distintos nombres como **eth0**, **en0**, u otros (el número 0 se refiere a la primera interfaz detectada en el sistema, ya que puede haber más).

La ventana que se le presentará, tendrá el siguiente aspecto y se puede seleccionar la interfaz que se desee (interface).



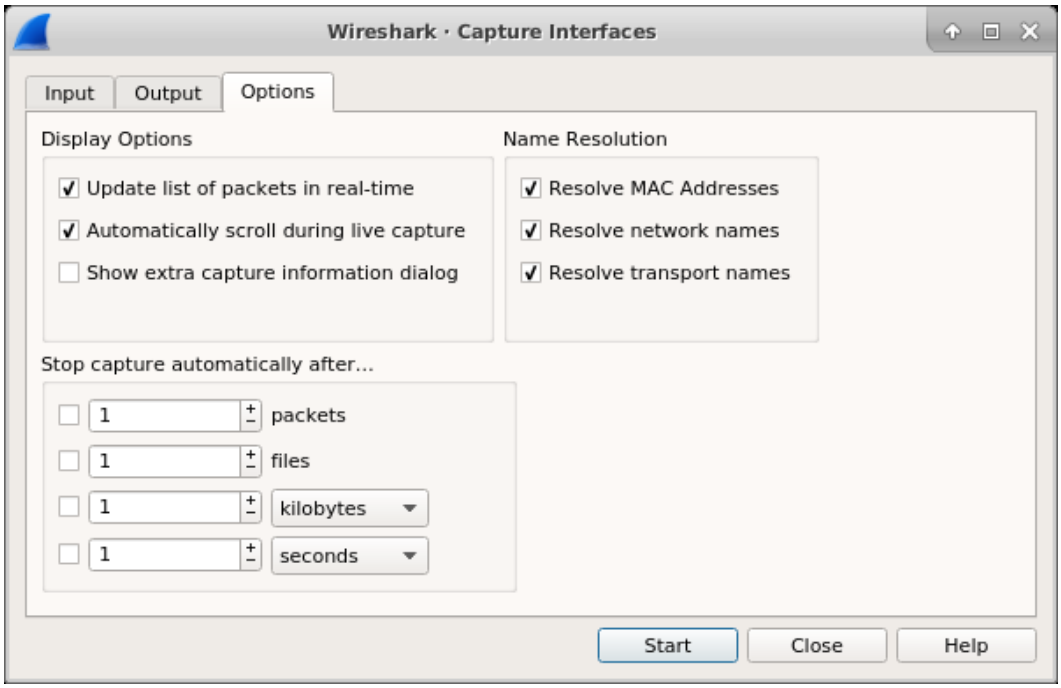
Active la siguiente opción si es que no lo estuviera ya:

- **Enable promiscuos mode on all interfaces**

La ventana ofrece varias pestañas. Vamos a la pestaña **Options** y activamos la siguiente opción:

- **Resolve network names**

Esto permitirá la captura de cualquier paquete y que sus campos de dirección se muestren como nombres en lugar de como números, siempre que sea posible. La ventana de opciones debería parecerse a la siguiente.



Importante: A lo largo de las prácticas con wireshark, si en algún momento pone un filtro en el que use un nombre en lugar de una dirección IP, y no le aparecen resultados, puede ser que no tenga activada la opción "Resolve network names". Si es así, lo puede comprobar fácilmente ya que en las columnas de Source y Destination sólo le aparecerán números, y no nombres.

2.5 Primera Captura

Una vez seleccionada la interfaz de red siga los siguientes pasos para realizar la primera captura.

En este primer caso vamos a utilizar una herramienta muy útil para trabajar en redes y ayudar a resolver problemas: **ping**. Esta aplicación permite comprobar si hay conectividad entre el equipo local y otro remoto basándose en el envío de paquetes al equipo remoto y la recepción de esos paquetes devueltos por el equipo remoto a modo de eco.

La aplicación ping se encuentra disponible en cualquier equipo y es accesible desde cualquier terminal de comandos. Antes de hacer la captura, asegúrese de que ha localizado el terminal de su ordenador y que está disponible la aplicación ping. Para ello tenga en cuenta lo siguiente:

- En equipos linux, el terminal se encuentra accesible desde el menú o mediante la ejecución de un *shell* (por ejemplo **/bin/bash**) en un entorno gráfico el programa se llama Terminal.
- En equipos windows, el terminal es accesible ejecutando el comando **cmd** o bien

desde el menu **inicio> todos los programas > accesorios > símbolo del sistema.** O bien Ejecutar comando (Tecla Windows+R) y ejecutar **cmd** o **powershell**.

Para hacer ping a la máquina **dns.google** sólo con cuatro intercambios de paquetes, ejecute los siguientes comandos, dependiendo del sistema operativo:

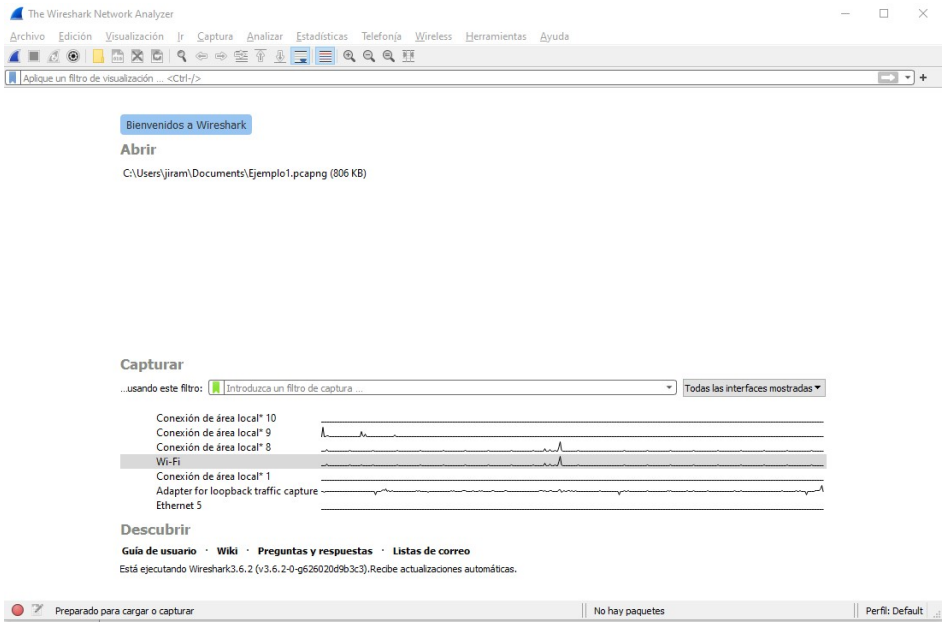
- Linux: **ping -c 4 dns.google**
- Windows: **ping -n 4 dns.google**

Como se puede imaginar, las opciones -c y -n sirven para enviar un número especificado de paquetes. Asegúrese de que el comando funciona y dedique un momento a interpretar los resultados del mismo.

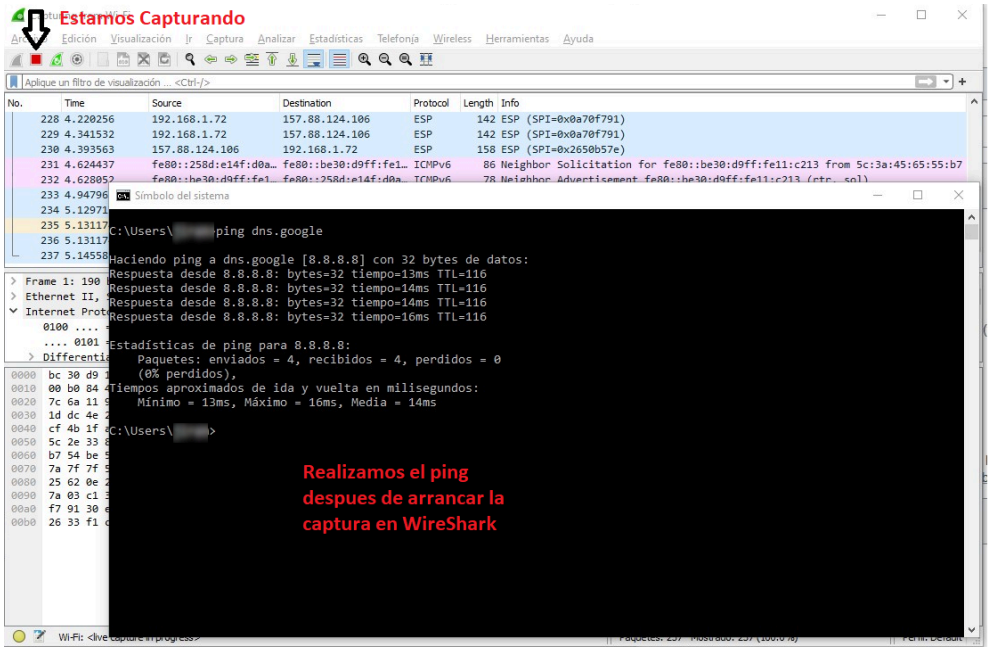
Nota: Si está conectado por eduroam, es probable que el ping no reciba respuesta porque en eduroam lo esté cortando un firewall por seguridad. No se preocupe, en ese caso en los pasos siguientes sólo verá la petición de ping, pero no la respuesta. Si quiere ver una respuesta al ping puede probar a lanzar el ping a la dirección IP de la puerta de enlace predeterminada (o default gateway) de su equipo. Recuerde que puede ver la puerta de enlace con los comandos *ipconfig* en windows y *netstat -rn* en linux.

Ahora vamos a proceder a la captura de los paquetes de red mientras se hace el ping. Siga los siguientes pasos:

1. Inicie la captura en el menu **Capture > Start**, o bien **Capture > Options**, seleccionar la interfaz que está usando (eth0, wiffi, Conexión Area Local, etc) y pulsar **Start** (también se puede hacer con el botón de acceso directo disponible (). Vea la siguiente captura donde hemos seleccionado la interface wifi y comenzamos la captura como hemos indicado.

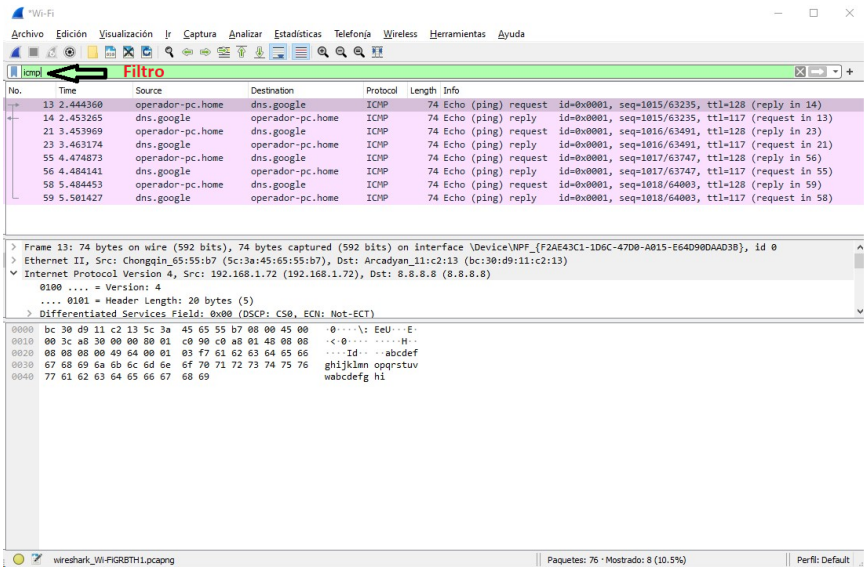


2. En el terminal, haga un ping (con cuatro paquetes será suficiente) a la dirección **dns.google**, tal y como ha hecho antes



3. Cuando obtenga la respuesta del servidor indicando que todo ha funcionado, pare la captura con la opción **Capture > Stop** o con el botón  .

Busque entre los paquetes los que se corresponden con el comando ping. En la siguiente imagen puede ver el filtro que hemos puesto para obtener los paquetes capturados del ping.



Observará que en los pocos segundos que ha durado la captura se han recogido una gran cantidad de paquetes. Para localizar los correspondientes al ping puede intentar varias estrategias, pero se sugiere que filtre los paquetes por el protocolo utilizado para hacer el ping, que en este caso es ICMP. Para ello escriba icmp en el cajetín del filtro (fíjese que aparece el siguiente mensaje: Apply a display filter ...).

Ahora sólo se deberían mostrar 8 paquetes, que son los correspondientes al ping realizado. Confirme esto y fíjese que están emparejados de 2 en 2 según las direcciones de origen y destino, uno va de su máquina local a dns.google y otro hace el camino contrario.

Si no es capaz de encontrar los paquetes, vuelva a repetir la captura con la petición (no es necesario que guarde los datos de la captura anterior). Para facilitar la búsqueda finalice la captura tan pronto como haya finalizado el ping. También puede reducir la cantidad de paquetes capturados desactivando el modo promiscuo, de modo que sólo se tengan en cuenta los paquetes destinados u originados en la interfaz elegida para la captura. Eso se puede hacer en la ventana **Capture > Options** o con el botón  .

2.6 Cargar fichero Wireshark parte1

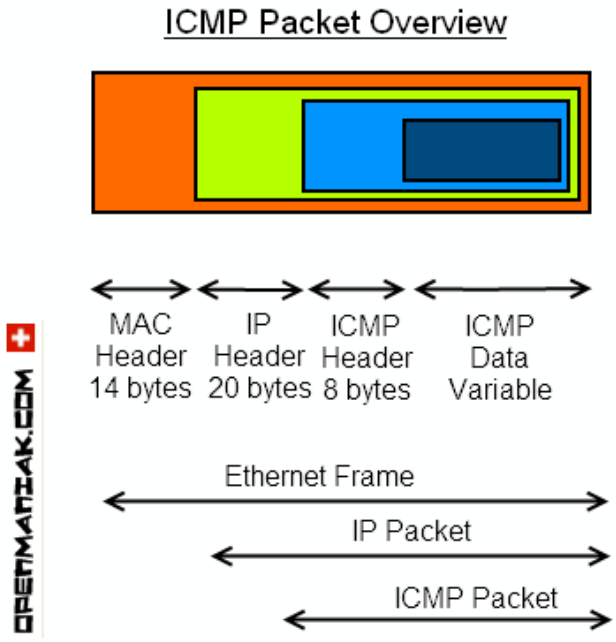
Una vez practicado con el programa descargue el siguiente fichero Parte1.pcapng[1]. Abra el fichero con el programa Wireshark. Este fichero contiene los paquetes de una captura de red. Lo usaremos para realizar filtros y búsquedas para responder las siguientes preguntas.

Aquí se incluyen tres preguntas aleatorias de sendos bancos de preguntas sobre filtros básicos en wireshark e identificación de parámetros de paquetes ping (ICMP echo request and reply).

2.7 Datos transmitidos en un paquete (payload)

En esta ocasión vamos a detenernos un poco en la relación entre el tamaño del mensaje y los datos que transporta. Para ello vamos a inspeccionar la información mostrada en los distintos niveles de información del paquete, correspondientes a cada capa de protocolo implicado en la transmisión del paquete, y nos fijaremos en el tamaño del paquete, en bytes.

Observe la siguiente figura para entender cómo está construido un paquete ICMP (por ejemplo, un ping o su respuesta). Los datos que se transportan, también llamados payload (*ICMP Data* en la figura), están ***encapsulados*** por las cabeceras de ICMP, de IP y de Ethernet (esto último aparece como MAC header en la figura).



[1] Los enlaces a ficheros con capturas están desactivados en el documento.

Vamos a ver esto con un ejemplo concreto.

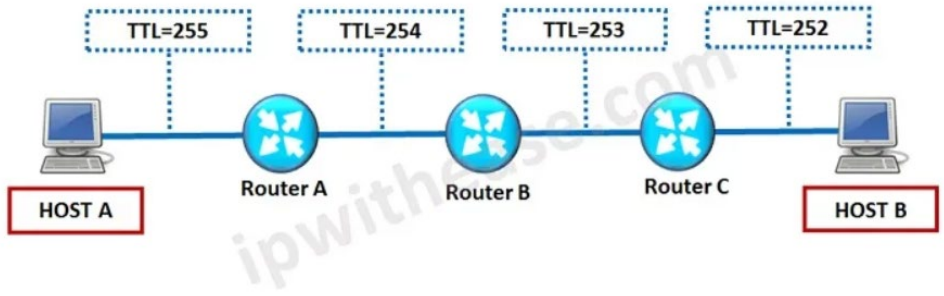
> Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre el tamaño de las cabeceras y el payload de un paquete.

2.8 Time to live (TTL)

En esta ocasión vamos a detenernos un poco en el concepto de TTL (Time to Live, tiempo de vida) de los paquetes.

Cuando un paquete de información es creado y enviado por internet, existe un riesgo de que éste continúe pasando de un router a otro de manera indefinida. Para evitar esta posibilidad, los paquetes están diseñados con una expiración llamada time-to-live o límite de saltos. El TTL también es útil para determinar cuánto tiempo un paquete ha estado en circulación y permitirle al remitente recibir la información acerca del camino de los paquetes a través de la internet.

Cada paquete tiene un campo en la cabecera IP, llamado TTL, donde es almacenado un valor numérico que determina cuánto le debería quedar al paquete para seguir en la red. En el caso de un ping suele ser 64 o 128 aunque al momento de ejecutar el comando podemos especificar el TTL con la opción -i *nº_de_saltos* para Windows y -t *nº_de_saltos* para Linux. Cada vez que un router recibe un paquete, le resta uno de la cuenta de TTL y entonces lo pasa a la próxima localización de la red. Si en algún punto el valor del TTL es igual a cero después de la resta, el router descartará el paquete y enviará un mensaje ICMP de error hacia el origen.



Veamos esto con un ejemplo concreto.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre el TTL de un paquete.

2.9 Filtrando en wireshark paquetes HTTP/HTTPS

En esta última captura, vamos a interesarnos por los paquetes que soportan una petición HTTP o HTTPS, que es el protocolo que gobierna el intercambio de solicitudes y respuestas web. Tan solo para que lo sepa, no es necesario que lo haga, se pueden generar peticiones web utilizando un navegador web (como firefox o chrome), o bien invocando el siguiente comando desde el terminal (en linux y Mac; en Windows habría que instalar previamente el programa wget):

wget --no-cache servidorweb.dominio.es

Descargue el fichero Parte2.pcapng desde este enlace[1]. Abra el fichero Parte2 en el programa Wireshark. En este fichero hemos realizado una serie de peticiones HTTP y HTTPS a distintos servidores.

Ahora tendrá que buscar los paquetes a los que se haga referencia para responder a la pregunta. Para ello recuerde poner filtros o combinación de filtros en el cajetín de filtros de la parte superior de wireshark, por ejemplo:

- tcp.port == 443 mostrará SOLO los paquetes que usen el puerto 443 esto es HTTPS
- ip.dst_host =="NOMBRE DNS DE MAQUINA" ejemplo: ip.dst_host == "www.uva.es" filtrará aquellos paquetes que tengan como destino www.uva.es
- ip.src_host =="NOMBRE DNS DE MAQUINA" ejemplo: ip.src_host =="www.uva.es" filtrará aquellos paquetes que tengan como origen www.uva.es
- Para que le funcione el filtro por nombre recuerde que tiene que tener activada la opción "Resolver nombres de host" en Captura > Opciones > Opciones
- ip.addr == IP ejemplo ip.addr == 8.8.8.8 mostrará todos los paquetes que tengan la ip 8.8.8.8 como origen o destino
- Se pueden usar operadores lógicos AND (&&) y OR (||) así podremos realizar filtrados más concretos, por ejemplo:

```
tcp.port == 443 && (ip.src_host == "nansa.infor.uva.es" &&
ip.dst_host=="bladerunner.infor.uva.es") Este filtro mostrará solo
los paquetes dirigidos o enviados al puerto 443 en que el origen sea
nansa.infor.uva.es y el destino bladerunner.infor.uva.es
```

[1] Los enlaces a ficheros con capturas están desactivados en el documento.

tcp.port == 443 &&(ip.addr == 157.88.124.104 && ip.addr==157.88.124.106) Este filtro mostrará solo los paquetes dirigidos o enviados al puerto 443 las direcciones IP de origen o destino sean 157.88.124.104 o 157.88.124.106.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre filtrado de paquetes HTTP/HTTPS.

> Aquí se incluye una pregunta final de autorreflexión y síntesis sobre la práctica realizada y los conocimientos adquiridos.

3. DNS y WHOIS

3.1 Introducción y Objetivos

En esta ocasión se le va a presentar un tema que tendrá que desarrollar por sí mismo. Durante el transcurso de esta actividad se le van a dar una serie de indicaciones básicas, a partir de las cuales tendrá que construir su propio conocimiento sobre el tema en cuestión y responder a las preguntas que se le vayan presentando.

Esta actividad requiere tener un equipo con la aplicación **Wireshark** para practicar lo que se vea en el asistente y sobre todo para cargar el archivo de captura de paquetes para poder responder al cuestionario.

En esta práctica vamos a profundizar en el conocimiento de DNS, sobre los mensajes que se envían y reciben entre los clientes y los servidores. También vislumbraremos la jerarquía de servidores DNS que responde a nuestras consultas.

Para seguir esta lección conviene revisar y tener a mano la sección correspondiente del libro de texto, a fin de refrescar los conceptos básicos de DNS. En particular, conviene tener claro los conceptos de servidor DNS local, caché de DNS, registros y mensajes DNS y el campo TYPE de los registros DNS.

3.2 DNS

DNS son las siglas de Domain Name System y se refiere a toda la infraestructura que existe en Internet para gestionar los nombres de dominio. Los nombres de dominio, o dominios a secas, son nombres asociados a las direcciones IP que facilitan el manejo de las mismas. Los dominios pueden tener subdominios, que permiten agrupar conjuntos de máquinas de forma más conveniente. Por ejemplo, **subred.mired.es** es un subdominio del dominio **mired.es**, dentro del cual puede encontrarse la máquina **xyz.subred.mired.es** con la dirección IP **123.123.123.123** .

DNS actúa de algún modo como las agendas de los teléfonos modernos, en los que en lugar de teclear el número de abonado al que se desea llamar, se elige un nombre y la agenda hace la traducción y los pasos necesarios para llamar a dicho contacto utilizando su número de teléfono.

Además de este servicio básico, DNS proporciona otros como:

- **alias de host**: lo que permite que una misma máquina pueda ser conocida por varios nombres.
- **alias de servidor de correo**: lo que permite averiguar la dirección del servidor de correo para un dominio.

- **distribución de carga**: lo que permite que varias direcciones IP estén asociadas con el mismo nombre de máquina.

DNS está compuesto por una base de datos distribuida compuesta por una **jerarquía de servidores** de nombres y por un **protocolo de consulta** a esa base de datos.

DNS está especificada entre otros, por los siguientes RFCs:

- RFC 1034, *Domain Names - Concepts and Facilities*
- RFC 1035, *Domain Names - Implementation and Specification*

Puesto que esos documentos resultan un poco duros de leer, quizás prefiera comenzar por la wikipedia. No dude en buscar más información por su cuenta.

El organismo implicado directamente en la coordinación de los servidores DNS, las direcciones IP y otros aspectos relacionados con protocolos es la Internet Assigned Numbers Authority (IANA). No pierda la oportunidad de completar su conocimiento sobre DNS y consulte la información que ofrece sobre el tema.

Una vez que haya localizado información suficiente, la haya leído e interiorizado, avance a las siguientes páginas donde se le plantearán distintos desafíos.

3.3 DNS: Base de Datos Distribuida Jerárquica

La base de datos de DNS es una base distribuida en la que participan distintos servidores, cada uno con distinta responsabilidad en el proceso.

A partir de la información que pueda encontrar sobre DNS (recuerde que en la página anterior se le proporcionó varias referencias, y puede consultar también los apuntes de teoría y especialmente el apartado "*A Distributed, Hierarchical Database*" del capítulo 2 del Kurose Ross) encuentre el papel de cada uno de los tipos de servidores DNS que forman parte de esa jerarquía:

- servidores raíz
- servidor de dominio de primer nivel (*Top Level Domain*, TLD)
- servidor con autoridad sobre un dominio (autoritativo)
- servidor de nombres local

Una vez que tenga claro esto, pase a responder la siguiente pregunta

> Aquí se incluyen dos preguntas aleatorias de sendos bancos de preguntas sobre tipos de servidores DNS.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre resoluciones de nombres directas e inversas.

3.4 Tipos de Registros DNS

La base de datos de DNS guarda diferentes tipos de registros sobre un dominio. Esta información es variada y comprende desde la dirección IP del dominio, hasta el servidor de nombres con autoridad sobre el mismo, pasando por los distintos alias con los que se puede conocer el mismo dominio.

Busque estos tipos de registros en el documento https://es.wikipedia.org/wiki/Anexo:Tipos_de_registros_DNS y responda a las siguientes preguntas.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre tipos de registros DNS.

3.5 DNS en Linux

En los sistemas Unix (linux, macOS, etc.) la configuración del servidor DNS de nombres por defecto (local) se centraliza mediante el archivo **/etc/resolv.conf**.

Este archivo puede ser editado manualmente, o bien a través de herramientas de configuración de red (con los privilegios de root necesarios).

Un vistazo al archivo nos permite determinar el servidor de nombres utilizado, además de otras informaciones relevantes asociadas.

Podemos conectarnos a la máquina **jair.lab.inf.uva.es** mediante SSH. Abra un terminal y teclee la siguiente línea de comandos:

```
ssh[nombre_de_usuario]@jair.lab.inf.uva.es
```

Nota: En el anterior comando, y en general, siempre que se explica un comando, las opciones del comando se indican entre corchetes, pero los corchetes no hay que escribirlos. Por ejemplo, si mi nombre de usuario es pericoper, el comando anterior sería: ssh pericoper@jair.lab.info.es

El nombre de usuario y la contraseña son los que utiliza para acceder a los equipos en la Escuela.

Una vez dentro de jair, vamos a acceder al contenido del archivo **resolv.conf** que está en el directorio **/etc** con el siguiente comando:

more /etc/resolv.conf

A continuación, se muestra la salida del comando **more /etc/resolv.conf** ejecutado en la máquina **jair.lab.inf.uva.es** (El comando **more** muestra el contenido del archivo por pantalla. Tambiénse puede utilizar el comando **cat** paraello.):

```
more /etc/resolv.conf
domain inf.uva.es
search inf.uva.es lab.inf.uva.es
nameserver 1.1.1.1
nameserver 157.88.109.249
nameserver 157.88.109.248
```

En la salida se puede observar que existen varios servidores DNS (etiqueta **nameserver**), nos centraremos en las direcciones **157.88.109.249** y **157.88.109.248**. También se puede observar que el dominio (**domain**) de jair es **inf.uva.es** y que el orden de búsqueda (**search**) de los dominios para completar nombres locales es **inf.uva.es** primero, y **lab.inf.uva.es** después. Esto último es útil porque permite utilizar nombres de máquina locales, sin dominio, que son más cortos y fáciles de manejar, y el sistema los completa cuando es necesario salir del dominio local.

Si consulta la información de este mismo archivo en su ordenador de laboratorio, verá que no coincide la información con la de jair, y esto es debido a variaciones en la configuración de los distintos sistemas operativos.

Deje la sesión abierta con **jair** ya que necesitaremos volver a esta configuración.

3.5.1 Comando dig

Existen varios comandos que permiten interrogar a DNS para que nos convierta una dirección IP en un nombre de dominio y viceversa, o para conseguir cualquier otro tipo de registro DNS. Algunos de ellos son los siguientes:

nslookup: Presente tanto en Unix/Linux como en Windows, aunque obsoleto desde el punto de vista técnico.

host: Alternativa a nslookup, presente en las distribuciones Unix/Linux. Resulta una herramienta útil para realizar consultas sencillas DNS.

En este caso vamos a utilizar la orden **dig**, que resulta ser un comando más potente y flexible para realizar consultas acerca de cualquier tipo de registro DNS. Por sus características es

utilizado por los administradores para resolver problemas con el DNS, y también con propósitos educativos, como es este caso.

El comando dig puede operar en modo interactivo o en modo batch (por lotes), tomando las operaciones desde un archivo y ejecutándolas secuencialmente. Cuando se invoca sin especificar ningún servidor de nombres, utiliza el establecido por defecto en el sistema, que usualmente está configurado en el archivo /etc/resolv.conf. Si se le invoca sin argumentos, realiza una consulta sobre los servidores DNS de la zona raíz (root).

Una consulta típica de dig es algo parecido a esto:

dig @[servidor] [nombre] [tipo]

donde:

servidor es el nombre o dirección IP del servidor de nombres al que consultar. Si no se especifica el servidor, utiliza la lista de servidores que encuentra en el archivo /etc/resolv.conf. El comando muestra por pantalla las respuestas obtenidas.

nombre es el nombre del dominio que se busca.

tipo indica el tipo de consulta a realizar: ANY, A, MX, SIG, NS, PTR, etc.

Abra un terminal en un sistema unix ya sea su máquina local o conectándose a jair.lab.inf.uva.es y ejecute el siguiente comando en su máquina personal linux o de los laboratorios:

```
dig
```

Como resultado obtendrá un conjunto de datos en respuesta a la consulta que acaba de realizar (sí, sorprendentemente ha realizado una consulta sobre el dominio raíz, que se indica por un punto ".") divididos en varias secciones:

- QUESTION SECTION: con la pregunta realizada. Observe que, aunque comentada por ";" el dominio sobre el que se responde es el raíz.
- ANSWER SECTION: con la lista de los 13 servidores de nombres raíz.
- ADDITIONAL SECTION: con información adicional a la respuesta, como las direcciones IPv4 e IPv6 de los servidores de nombres anteriores.

En el caso de consultar sobre un host concreto, el contenido de las secciones se modifica un poco y puede aparecer una sección más:

- AUTHORITY SECTION: con la información sobre los servidores de nombres con autoridad sobre el dominio al que pertenece el host.

Para más información acceder a la página de manual de dig (sección 1) tecleando la orden en un terminal o en la consola del sistema:

```
man 1 dig
```

Dedique unos minutos a abrir un terminal y consultar el manual sobre el comando dig. También puede obtener una versión reducida de las opciones del comando consultando la ayuda que proporciona a través del mismo si teclea la siguiente orden:

```
dig -h
```

Familiarícese con el comando consultando, por ejemplo, la dirección del dominio inf.uva.es antes de avanzar a la siguiente página.

3.6 Descubrimiento del dominio infor.uva.es

Para averiguarlo teclee el siguiente comando preferiblemente en jair (o también en un terminal de una máquina linux del laboratorio):

- **$ dig @157.88.109.248 infor.uva.es ANY**

Al añadir el argumento ANY, está consultado toda la información que se tiene de ese dominio.

3.7 Resolución Inversa

DNS, además de proporcionar la resolución de nombres en direcciones IP, también da la posibilidad de averiguar el nombre de un dominio conocida su dirección IP; lo que se denomina resolución inversa. Para ello DNS almacena las direcciones IP como si fuesen hostnames de un dominio ficticio. Ese dominio es el dominio **in-addr.arpa**. Así, al hacer la consulta inversa preguntando por una IP, busca en su base de datos de forma similar a cuando se hace una consulta directa, pero en este caso busca el nombre que se corresponda con [dirección_IP].in-addr.arpa y la respuesta será el valor asociado a ese nombre ficticio,

que contendrá el nombre de dominio correspondiente a la dirección IP.. Para esto se vale de un tipo de registro **PTR** que indica esa resolución inversa.

La sintaxis del comando dig para realizar una resolución inversa es la siguiente:

- **$ dig -x *[dirección_IP_a_resolver]***

Prueba a ejecutar este comando con la IP de infor.uva.es. La respuesta se da en la sección ANSWER; fíjese en el registro **PTR**. Observe que el dominio por el que se ha consultado se compone de la dirección IP inversa, de derecha a izquierda, y del dominio **in-addr-arpa**.

> Aquí se incluyen dos preguntas aleatorias de sendos bancos de preguntas sobre resultados de ejecuciones del comando dig.

3.8 Capturar y analizar el tráfico DNS

Una vez que nos hemos familiarizado con la herramienta dig, estamos en disposición de profundizar en nuestro conocimiento de DNS. Para ello vamos a realizar unas consultas DNS y capturar los paquetes correspondientes.

3.8.1 Pruebas previas de generación y captura de paquetes DNS

Primero practicaremos unos minutos capturando con Wireshark paquetes de consultas y respuestas DNS. Para ello, salga de jair y siga los siguientes pasos.

1. Abra un terminal nuevo en su máquina local y prepare el comando que se indica a continuación (**pero no lo ejecute todavía**) para consultar la dirección de *www.uva.es* al servidor de nombres *ns1.infor.uva.es*. Esto último asegura que la consulta es respondida por ese servidor y no se consulta al registro de información dns que almacena localmente el host (caché), o a otro servidor externo como es el 1.1.1.1, lo que podría dificultar el análisis del tráfico con Wireshark.
   - Linux/Unix/Mac: **dig @ns1.infor.uva.es www.uva.es**
   - Windows: **nslookup www.uva.es ns1.infor.uva.es**
2. Abra Wireshark y filtre los mensajes de consulta y respuesta DNS originados o destinados a la dirección IP de su máquina, introduciendo en el filtro "**dns**".

Inicie la captura sobre la interfaz de red que le corresponda en el caso de los equipos del laboratorio la Ethernet.

Ejecute el comando indicado en el punto 1 en el terminal y espere a que finalice.

Espere unos segundos y pare la captura de paquetes en Wireshark.

A continuación, aprenda a filtrar y analizar la información capturada por el Wireshark: encuentre las consultas y respuestas DNS que han generado el comando que ha ejecutado, e investigue la información que aparece en cada paquete. Dedique unos minutos, pero no muchos, y continúe con la siguiente página.

3.8.2 Análisis de otro fichero con captura de wireshark

A partir de ahora trabajaremos con una captura guardada en un fichero que se descargará a continuación. **No realice los ejercicios siguientes con la captura que ha realizado en el paso anterior**, hay que realizarlos con la captura que le vamos a pasar a continuación.

Vamos ahora a trabajar con Wireshark y el DNS. En el archivo que puede descargar de este link[1] hemos realizado una captura de tráfico de un equipo. En él, hay varias peticiones a servidores DNS.

En las siguientes preguntas tendrá que buscar los paquetes a los que se haga referencia para responder a la pregunta. Para ello recuerde poner filtros o combinación de filtros, por ejemplo:

- tcp.port == 443 mostrará SOLO los paquetes que usen el puerto 443 esto es HTTPS
- ip.dst_host =="NOMBRE DNS DE MAQUINA" ejemplo: ip.dst_host =="www.uva.es" filtrará aquellos paquetes que tengan como destino www.uva.es
- ip.src_host =="NOMBRE DNS DE MAQUINA" ejemplo: ip.src_host =="www.uva.es" filtrará aquellos paquetes que tengan como origen www.uva.es
- ip.addr == IP ejemplo ip.addr == 8.8.8.8 mostrará todos los paquetes que tengan la ip 8.8.8.8 como origen o destino
- dns filtra los paquetes que usen el protocolo dns

Recuerde que se pueden usar operadores and (&&) y or (||) así podremos realizar filtrados más concretos.

Es importante que realice correctamente los filtros para contestar las siguientes preguntas sobre el paquete concreto.

A continuación responda a las siguientes preguntas, realizando en cada una el filtro de paquetes que necesite.

> Aquí se incluyen cuatro preguntas aleatorias de sendos bancos de preguntas que requieran filtrar por el protocolo DNS, host origen y destino, y en las que se pregunte por valores de campos de las cabeceras de distintas capas de protocolos, como el puerto TCP/UDP o el tipo de consulta DNS.

[1] Los enlaces a ficheros con capturas están desactivados en el documento.

3.9 WHOIS

Existe otra forma de consultar información sobre un dominio, en este caso la información es de tipo administrativo. El servicio **whois** proporciona información sobre quién es el propietario del mismo, quién ha sido el registrador, la fecha de creación y expiración de la reserva del dominio y algunos detalles técnicos, como los servidores del mismo.

Una explicación concisa sobre el servicio se puede encontrar en http://en.wikipedia.org/wiki/Whois.

Una buena forma de acercarse al tema del registro de los dominios es visitar http://www.dominios.es/ que es el organismo encargado de gestionar el dominio **.es** . Plantéese qué pasos debería dar para registrar su propio dominio y cuáles son los actores implicados en el mismo.

Existen versiones web del servicio whois, pero en este caso vamos a investigar las posibilidades del comando homónimo. Aprenda sobre el manejo del mismo consultando el manual o bien la ayuda del comando con los respectivos comandos:

- **man whois**
- **whois -h**

Si no dispusiera del comando en su sistema (porque no estuviera instalado, por ejemplo) puede utilizar un servicio accesible en la Web como por ejemplo

- http://whois.icann.org/

Experimente con distintas consultas. Resulta preferible que se centre en consultas sobre dominios **.com**, ya que por ejemplo, los dominios **.es** tienen restringido este servicio por motivos de seguridad.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas que requiera obtener la información de un dominio en https://whois.icann.org y responder a alguna pregunta sobre dicha información

> Aquí se incluye una pregunta final de autorreflexión y síntesis sobre la práctica realizada y los conocimientos adquiridos.

4. Capa de transporte

4.1 Introducción y Objetivos

En esta ocasión se le va a presentar un tema que tendrá que desarrollar por sí mismo. Durante el transcurso de esta actividad se le van a dar una serie de indicaciones básicas, a partir de las cuales tendrá que construir su propio conocimiento sobre el tema en cuestión y responder a las preguntas que se le vayan presentando.

Esta actividad requiere tener un equipo con la aplicación **Wireshark** para practicar lo que se vea en el asistente y sobre todo para cargar el archivo de captura de paquetes para poder responder al cuestionario.

En esta práctica vamos a profundizar en el conocimiento de conceptos básicos de la capa de Transporte y aprenderemos a seguir flujos tcp en wireshark, a distinguir el three way handshake, lo que son números de secuencia, ACK, etc.

Para seguir esta lección conviene revisar y tener a mano la sección correspondiente del libro de texto, a fin de refrescar los conceptos básicos de la capa de Transporte.

4.2 Ethernet la tupla dirección puerto (socket)

Según la Wikipedia la **capa de aplicación** ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y protocolos de transferencia de archivos (FTP).

Las aplicaciones utilizan la **capa de transporte** para enviar y recibir datos de una forma eficiente, confiable y económica. Merece la pena echar un vistazo rápido al apartado de servicios de la entrada en Wikipedia correspondiente a la capa de transporte. Dedica un par de minutos a ello y luego continúa leyendo.

Hay dos tipos de servicio en la capa de transporte: orientado a conexión, y no orientado a conexión.

- En el **orientado a conexión** primero hay un establecimiento de sesión entre los extremos, luego se transmiten datos por dicha sesión, y finalmente se libera la sesión. Generalmente, en este tipo de servicio interesa asegurarse de que todos los paquetes llegan correctamente, por lo que se usan números de secuencia para identificarlos, y los extremos envían un mensaje de reconocimiento al otro lado para avisar de que le han llegado, y en caso de que no sea así, se retransmiten los paquetes. Ejemplos de protocolos que ofrecen este tipo de servicio son TCP o SCTP.
- En el **no orientado a conexión** se trata cada paquete individualmente, y normalmente no es tan importante asegurarse de que el paquete ha llegado, y es más importante la

velocidad, por lo que no suele haber comprobación de si han llegado. UDP es un protocolo de capa de transporte no orientado a conexión.

Distintas aplicaciones usarán un protocolo u otro en función de las necesidades que tengan.

En esta práctica nos centraremos principalmente en TCP. Algunas aplicaciones, como los navegadores de internet, usan TCP en la capa de transporte para transmitir datos. Cada conexión se debe identificar siempre claramente mediante dos puntos terminales definidos (cliente y servidor). En este contexto, qué lado desempeña el papel de cliente y cuál el de servidor es indiferente. Lo que importa es que el software TCP cuente con una pareja (también denominada “2-tupla” o “socket”) ordenada de dirección IP y puerto TCP en cada punto terminal. La dirección IP identifica el extremo remoto en la capa de red, y el puerto identifica la aplicación en el extremo remoto.

En esta ocasión vamos a realizar filtros en Wireshark para averiguar qué protocolo de transporte, y puertos origen o destino utilizan las distintas aplicaciones.

Vamos ahora a trabajar con Wireshark. En el archivo que puede descargar de este link[1] hemos realizado una captura de tráfico de un equipo. En él, hay varias peticiones a servidores usando distintos protocolos de aplicación.

Ahora tendrá que buscar los paquetes a los que se haga referencia para responder a la pregunta para ello recuerde poner filtros o combinación de filtros, por ejemplo:

- tcp.port == 443 mostrará SOLO los paquetes que usen el puerto 443 esto es HTTPS
- ip.dst_host =="NOMBRE DNS DE MAQUINA" ejemplo: ip.dst_host =="www.uva.es" filtrará aquellos paquetes que tengan como destino www.uva.es
- ip.src_host =="NOMBRE DNS DE MAQUINA" ejemplo: ip.src_host =="www.uva.es" filtrará aquellos paquetes que tengan como origen www.uva.es
- ip.addr == IP ejemplo ip.addr == 8.8.8.8 mostrará todos los paquetes que tengan la ip 8.8.8.8 como origen o destino
- dns filtra los paquetes que usen el protocolo de aplicación dns
- smb filtra los paquetes que usen el protocolo de aplicación samba
- ssh filtra los paquetes que usen el protocolo de aplicación ssh
- syslog filtra los paquetes que usen el protocolo de aplicación syslog
- snmp filtra los paquetes que usen el protocolo de aplicación snmp
- smtp filtra los paquetes que usen el protocolo de aplicación smtp

[1] Los enlaces a ficheros con capturas están desactivados en el documento.

- whois filtra los paquetes que usen el protocolo de aplicación whois
- ssdp filtra los paquetes que usen el protocolo de aplicación ssdp
- rsh filtra los paquetes que usen el protocolo de aplicación rsh
- quic filtra los paquetes que usen el protocolo de aplicación quic
- mdns filtra los paquetes que usen el protocolo de aplicación mdns
- http filtra los paquetes que usen el protocolo de aplicación http
- dhcp filtra los paquetes que usen el protocolo de aplicación dhcp

Recuerde que se pueden usar operadores and (&&) y or (||) así podremos realizar filtrados más concretos.

Es importante realice correctamente los filtros para contestar a las siguientes preguntas sobre el paquete concreto.

Responda a las siguientes preguntas.

Aquí se incluyen cuatro preguntas aleatorias de sendos bancos de preguntas que requieran filtrar por distintos campos, como protocolo, host y/o dirección IP, y en las que se pregunte por ejemplo, por el protocolo de la capa de transporte que se usa, el puerto, la dirección IP o el hostname.

4.3 Triple apretón de manos (Three Way Handshake)

Para que el establecimiento de una conexión TCP válida sea posible, ambos puntos terminales deben contar con una dirección IP unívoca (IPv4 o IPv6) y deben haber declarado y habilitado el puerto deseado para la transmisión de datos. Mientras que la dirección IP funciona como característica de identificación del punto terminal, el puerto sirve para que el sistema operativo pueda asignar las conexiones a las aplicaciones adecuadas de servidor y de cliente.

Ahora tendrá que buscar los paquetes a los que se haga referencia para responder a la pregunta para ello recuerde poner filtros o combinación de filtros, por ejemplo:

- tcp.port == 443 mostrará SOLO los paquetes que usen el puerto 443 esto es HTTPS
- ip.dst_host =="NOMBRE DNS DE MAQUINA" ejemplo: ip.dst_host =="www.uva.es" filtrará aquellos paquetes que tengan como destino www.uva.es

- ip.src_host =="NOMBRE DNS DE MAQUINA" ejemplo: ip.src_host =="www.uva.es" filtrará aquellos paquetes que tengan como origen www.uva.es
- ip.addr == IP ejemplo ip.addr == 8.8.8.8 mostrará todos los paquetes que tengan la ip 8.8.8.8 como origen o destino
- dns filtra los paquetes que usen el protocolo de aplicación dns
- smb filtra los paquetes que usen el protocolo de aplicaciónsamba
- ssh filtra los paquetes que usen el protocolo de aplicación smb
- syslog filtra los paquetes que usen el protocolo de aplicación syslog
- snmp filtra los paquetes que usen el protocolo de aplicación snmp
- smtp filtra los paquetes que usen el protocolo de aplicación smtp
- whois filtra los paquetes que usen el protocolo de aplicación whois
- ssdp filtra los paquetes que usen el protocolo de aplicación ssdp
- rsh filtra los paquetes que usen el protocolo de aplicación rsh
- quic filtra los paquetes que usen el protocolo de aplicación quic
- mdns filtra los paquetes que usen el protocolo de aplicación mdns
- http filtra los paquetes que usen el protocolo de aplicación http
- dhcp filtra los paquetes que usen el protocolo de aplicación dhcp

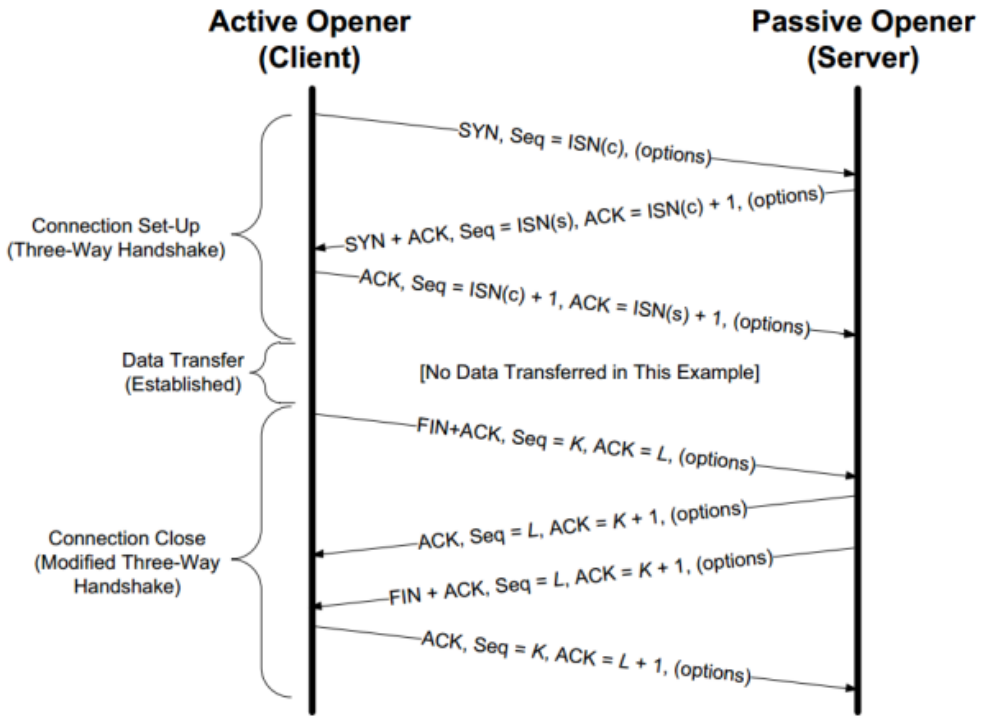
A los filtros aprendidos anteriormente ahora necesitaremos también los que hagan referencia a los flag de una conexión TCP:

- tcp.flags.syn == 1 filtrará los paquetes que tengan el flag syn activado
- tcp.flags.ack == 1 filtrará los paquetes que tengan el flag ack activado
- tcp.ack filtrará los paquetes que sean ack
- tcp.flags==0x12 permite filtrar por el valor del campo, este ejemplo filtra los paquetes que tienen ACK y SYN

Una vez que hemos aprendido los nuevos filtros vamos a localizar los paquetes Three Way Handshake de una conexión. En TCP el establecimiento de la conexión se realiza en tres pasos, en donde ambos puntos terminales se envían un paquete indicando que quieren establecer la conexión (activando un flag llamado SYN en la cabecera TCP), y reconocen el paquete del otro extremo que contenía el flag SYN, con un ACK.

Mientras se transmiten datos cada extremo sigue enviando ACKs para reconocer la recepción de paquetes.

La finalización de la conexión se realiza mediante la activación del flag FIN de la cabecera TCP. Para dar por finalizada la conexión, ambos extremos tienen que mandar un paquete con el flag de FIN activo, y reconocer el paquete del otro extremo con dicho flag.



Fuente: *https://notes.shichao.io/tcpv1/ch13/*

Vamos ahora a trabajar con Wireshark, con el mismo archivo que antes, que puede descargar de este link[1].

Es importante que realice correctamente el filtro que corresponda para contestar a las siguientes preguntas sobre el paquete concreto.

> Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren filtrar el three way handshake de TCP, y también sobre el ACK y hasta qué paquete reconoce el ACK.

4.4 Fragmentación, MSS y MTU

En el inicio de una conexión TCP se negocian las capacidades que tienen los extremos de la conexión. Para ello se usa el campo Options de la cabecera TCP. Uno de los parámetros de este campo es el **Tamaño Máximo de Segmento** (*Maximum Segment Size* - **MSS**). Es el tamaño más grande de datos, especificado en bytes, que un dispositivo de comunicaciones

[1] Los enlaces a ficheros con capturas están desactivados en el documento.

puede recibir en un único trozo, sin fragmentar. Así, en el inicio de la conexión TCP (three way handshake) cada extremo informa al otro del tamaño máximo de paquete que puede recibir.

Para una comunicación óptima, la suma del número de bytes del segmento de datos y la cabecera debe ser menor que el número de bytes de la unidad máxima de transferencia (MTU) de la red, ya que si es mayor, el paquete deberá ser fragmentado, y posteriormente reconstruido.

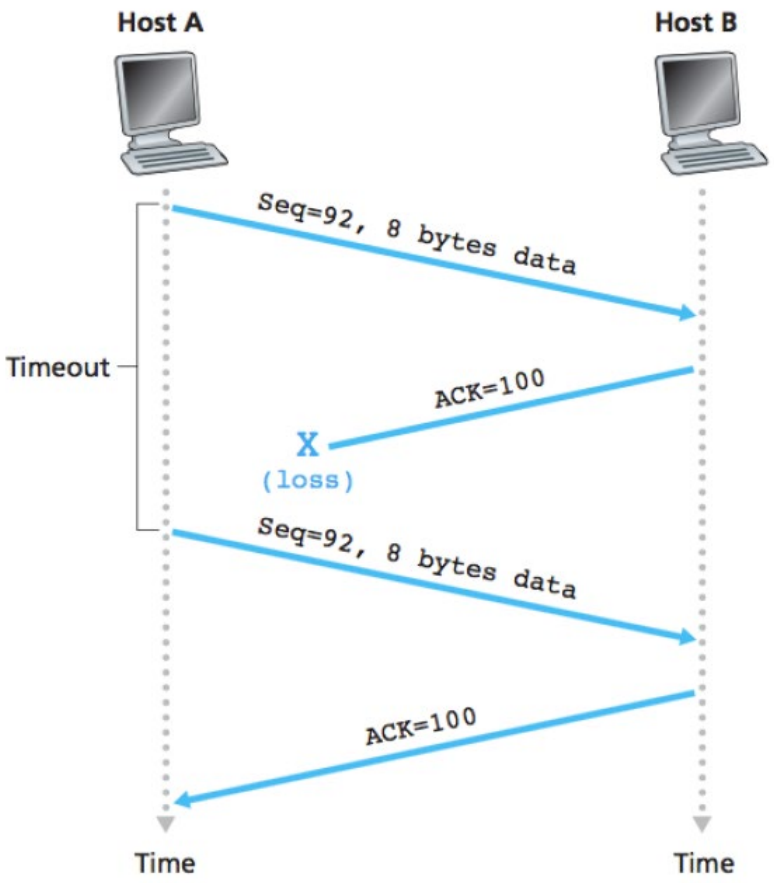
4.5 Retransmisión, RTT y RTO en TCP

La retransmisión de paquetes de host es la función de recuperación de errores más básica de TCP y su objetivo es evitar la pérdida de paquetes.
Hay muchas razones posibles para la pérdida de paquetes, incluida la falla de la aplicación, la sobrecarga del equipo de enrutamiento o el tiempo de inactividad temporal del servicio. La velocidad del nivel del mensaje es muy alta y, por lo general, la pérdida del mensaje es temporal, por lo que es muy importante que TCP pueda detectar y recuperar la pérdida del mensaje.
El mecanismo principal para determinar si hay que retransmitir un paquete es el temporizador de retransmisión (RTO). RFC2988 describe RTO así: “The Transmission Control Protocol (TCP) uses a retransmission timer to ensure data delivery in the absence of any feedback from the remote data receiver. The duration of this timer is referred to as RTO (retransmission timeout).”

Cuando se transmite un mensaje utilizando TCP, el temporizador de retransmisión comienza y el temporizador se detiene cuando se recibe un ACK. El tiempo desde que se envía un mensaje hasta que se recibe un ACK se denomina tiempo de ida y vuelta (round trip time, RTT).

RTT (tiempo de ida y vuelta) se compone de tres partes: tiempo de propagación del enlace (retraso de propagación), tiempo de procesamiento del sistema final, retraso de espera y procesamiento (retraso de espera) en el caché del enrutador. Entre ellos, los valores de las dos primeras partes son relativamente fijos para una conexión TCP, y el tiempo de espera y procesamiento en la memoria caché del enrutador cambiará a medida que cambie la congestión de la red. Por lo tanto, el cambio de RTT refleja el grado de congestión de la red hasta cierto punto.

El valor de RTO lo va actualizando el transmisor permanentemente en función de la medida del RTT, calculando un promedio de RTT de varios paquetes. Si un paquete se pierde, vencerá el temporizador, y entonces el transmisor lo retransmitirá. La siguiente figura ilustra el proceso de retransmisión de TCP.



Fuente: James F. Kurose, Keith W. Ross. Computer networking: A top-down approach. 6th ed. Pearson. 2013

Aquí se incluyen dos preguntas aleatorias de sendos bancos de preguntas que requieren filtrar paquetes con el flag SYN activo e identificar el MSS, y también sobre el RTO de algún paquete.

4.6 Estados de la conexión TCP

A veces aparecen problemas que afectan a nuestras conexiones de red. Esos fallos pueden ser simplemente por una mala configuración, algún driver sin actualizar, algún dispositivo que funciona mal o algún problema a nivel de sistema. Podemos hacer uso de diferentes herramientas y métodos para comprobar que todo funciona correctamente.

Netstat es una herramienta que podemos utilizar a través de la línea de comandos. Nos permite monitorizar las redes y también poder solucionar determinados problemas que

puedan surgir. Nos ofrece información en detalle de las conexiones de nuestro dispositivo a través de la terminal.

Esta herramienta está integrada tanto en Windows como en Linux. Es muy antigua, ya que desde principios de la década de 1990 está disponible tanto en Unix como en el SO de Microsoft (a partir de la versión 3.119).
Para utilizar Netstat en Windows o en Linux debemos ir a la línea de comandos. Para ello en windows vamos a Inicio, escribimos CMD y lo ejecutamos en modo de administrador y en Linux abrimos un terminal. Posteriormente simplemente tenemos que escribir netstat y darle a Enter. Nos aparecerá listado con las conexiones establecidas y su estado. Para que el comando netstat no tarde mucho por la resolución de nombres recomendamos ejecutar ***netstat -n***

Los parámetros más comunes del comando son:

- Netstat –a: nos permite conocer todas las redes que están activas o inactivas en un momento dado. Así lograremos detectar posibles problemas que afecten a una red.
- Netstat –e: en este caso podemos ver estadísticas sobre los paquetes de red entrantes y salientes en una tarjeta de red.
- Netstat –f: muestra el nombre de dominio completo de direcciones remotas.
- Netstat –n: este comando, a diferencia del anterior, muestra los números de puerto en lugar de los nombres.
- Netstat –o: muestra el ID de cada proceso en cada conexión.
- Netstat –p X: con este comando podemos filtrar conexiones según el protocolo (TCP, UDP, tcpv6 o tcpv4. X=TCP, UDP… el protocolo que queramos. Por ejemplo sería netstat –p TCP.
- Netstat –q: consultar los puertos de escucha y de no escucha vinculados.
- Netstat –s: muestra las estadísticas de grupo por protocolo. Así podremos clasificar las redes según los protocolos disponibles: TCP, UDP, ICMP, IPv4 o IPv6.
- Netstat –r: este comando nos muestra la tabla de enrutamiento de la red actual.
- Netstat –t: ofrece información sobre las conexiones en estado de descarga.Netstat –x: en este caso podemos obtener información sobre todas las conexiones NetworkDirect.

Ahora que conocemos el comando netstat responda a la siguiente pregunta.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas que requiere conectarse a una máquina Linux por ssh, ejecutar netstat -an, y responder sobre el estado de las conexiones tcp.

> Aquí se incluye una pregunta final de autorreflexión y síntesis sobre la práctica realizada y los conocimientos adquiridos.

5. Primeros pasos con el Packet Tracer

En esta ocasión vamos a aprender a utilizar una herramienta que nos será muy útil para diseñar y simular redes de computadoras. Esta herramienta se llama Packet Tracer (PT) y es un elemento clave de la estrategia del programa de certificación de Cisco.

PT nos proporciona un entorno en el que poder diseñar, configurar y probar el funcionamiento de las redes, permitiendo observar y analizar los paquetes que se intercambian. Las opciones de elementos que se pueden integrar en los diseños y simulaciones son muy variadas y reproducen los dispositivos más comunes en las redes. En este primer contacto con PT los objetivos son:

- Aprender a iniciar el programa
- Distinguir los paneles de la interfaz
- Realizar tareas sencillas de observación de una red

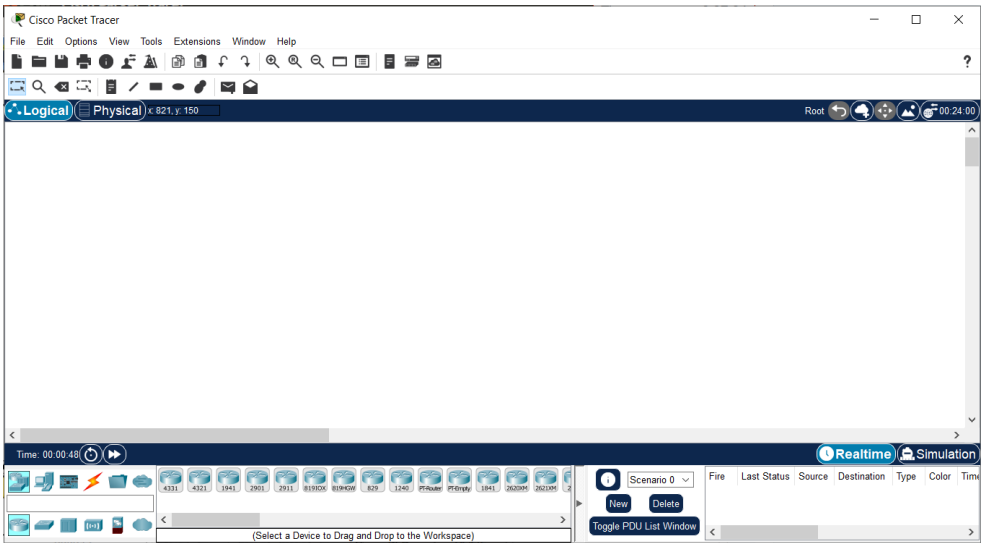
5.1 La aplicación PT y sus distintos paneles

La herramienta **Packet Tracer** está instalada en los PCs del laboratorio, o debería habérsela instalado con antelación en su portátil si lo va usar. Es necesario **registrarse** para poder usar Packet Tracer, ya bien sea en la instalación del laboratorio o en vuestro portátil. Debería haberse registrado con antelación para no perder tiempo en el laboratorio. De cualquier forma, puede consultar el aviso enviado con las instrucciones de registro e instalación.

Una vez que se complete la instalación, inicie la ejecución de Packet Tracer. Le pedirá que **inicie sesión** usando el usuario y contraseña con el que se registró antes en la web. Si tiene problemas para conseguir abrir la cuenta en ese momento, siempre se puede acceder como invitado (Guest) seleccionando la opción que se presenta pasado un breve intervalo de tiempo en la parte inferior derecha, aunque esta opción de uso presenta limitaciones en la grabación de las simulaciones.

Es muy recomendable que realice por su cuenta (fuera de clase) alguno de los cursos introductorios de Packet Tracer que se pueden encontrar en la misma web en 'Courses > Packet Tracer'. Son interesantes y se aprende mucho sobre el manejo de la herramienta y sobre redes.

Una vez que ha conseguido autenticarse en la aplicación, debería obtener una ventana como la que aparece en la siguiente figura (el contenido puede variar según la plataforma y versiones).

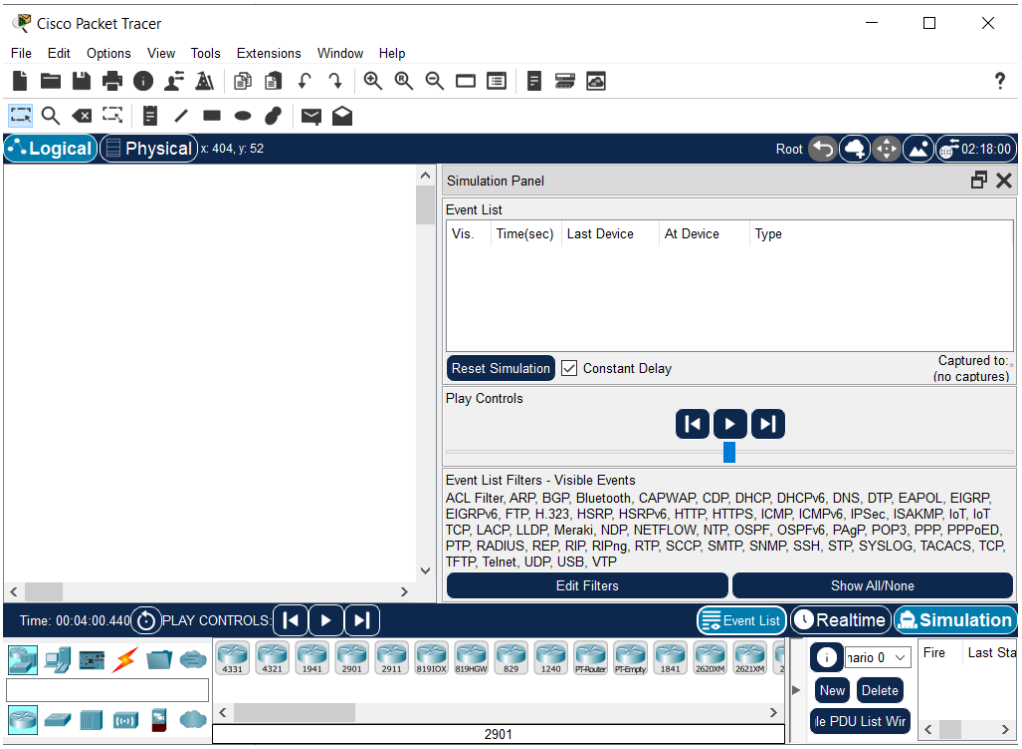


En la aplicación se pueden distinguir cuatro paneles y dos modos de funcionamiento.

Los paneles son los siguientes:

1. **Tapiz**: ocupa la parte principal de la ventana. En él se colocarán los elementos que compondrán la red.
2. **Paleta de herramientas**: dispuesta arriba agrupa herramientas de uso común para seleccionar los elementos de la red, así como para realizar operaciones comunes como hacer un ping entre equipos ( ).
3. **Catálogo de elementos**: en la parte inferior izquierda se muestran los distintos elementos que pueden formar parte de la red agrupados por familias. En la figura están seleccionados los routers y en la parte derecha del panel se muestran las distintas opciones de routers disponibles.
4. **Ejecución**. Es el panel situado en la parte inferior derecha se pueden seguir la evolución de las distintas acciones que se realizan en la red. Esta evolución puede ser observada en tiempo real o en modo simulación.

Inicialmente, PT se coloca en modo de tiempo real (**Real Time**), lo que nos permite observar el comportamiento de la red e interactuar en ella de un modo muy similar a una red funcionando en la realidad. A veces resulta más interesante poder controlar el tiempo, parándolo, avanzando o retrocediendo, de modo que podamos observar con más detalle la sucesión de paquetes que se intercambian entre los dispositivos. Para ello debemos activar el modo simulación (**Simulation**) picando en el botón correspondiente Simulation que aparece a la derecha en la banda azul inferior, que nos mostrará la siguiente figura.



En el panel de simulación se mostrarán los distintos paquetes, que serán los que se muevan por el tapiz. Estos paquetes pueden ser seleccionados e inspeccionados en todas sus capas.

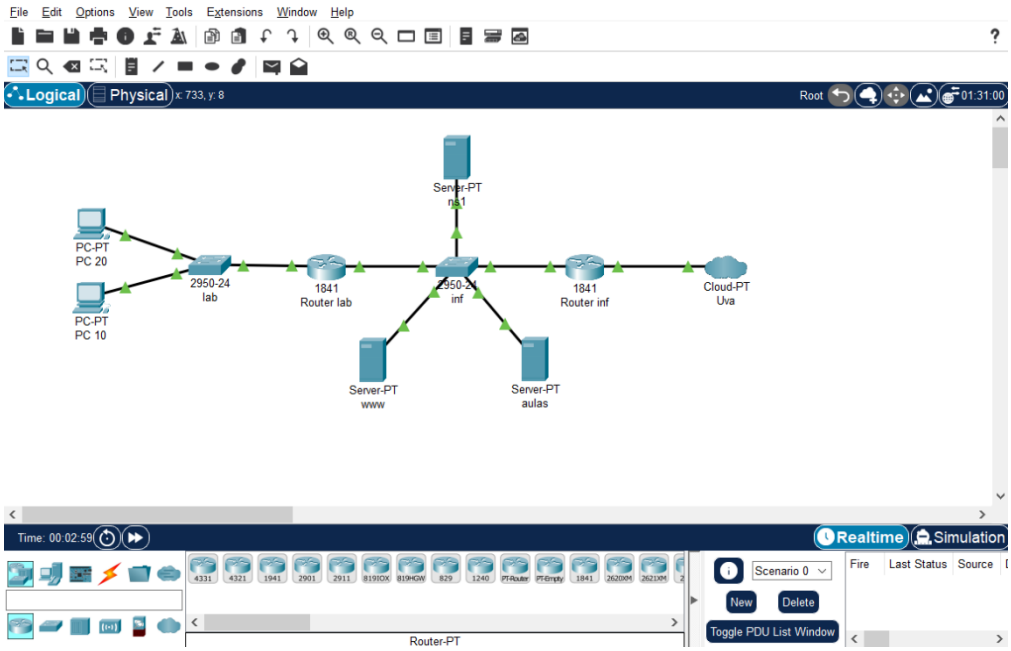
En el modo simulación se puede avanzar el tiempo paso a paso (Capture/Forward), retroceder (Back) y hacer que la simulación avance automáticamente paso a paso (Play).

También se pueden seleccionar los protocolos cuyos paquetes se desean observar (Edit Filters) o bien tener el conjunto completo de protocolos (Show All).

Dedique unos minutos descubrir las distintas partes del PT y las posibilidades que presentan.

5.2 Simulación de la red de la escuela

En esta ocasión vamos a trabajar con un modelo que simula la red de la Escuela tal como el que aparece en la figura.



En ella se pueden ver los dos dominios existentes, tanto **lab** como **inf.**

También están representados dos de los PCs de los laboratorios y algunos servidores web y DNS de la Escuela. Además están dos de los routers que se encargan de encaminar el tráfico en las redes existentes y dos switches que por ahora sólo debemos considerar como elementos a los que se conectan los host y los routers de cada red y permiten que los paquetes pasen de una red a otra. En el extremo derecho está representada la red de la UVa en forma de nube. Por ahora ese elemento sólo está para completar la red y que no aparezca como desconectada del mundo.

Ahora abra el modelo en su PT descargando el archivo lab_fi_uva.pkt[1].

Puede echar un vistazo a la configuración de los elementos pasando el cursor por cada uno de los dispositivos y dejando que se muestre el resumen de su configuración. Compruebe las configuraciones de los hosts y del DNS en el modelo. Para comprobarlo, por ejemplo, pique sobre **PC10** y vaya a la pestaña **config**. Se le mostrarán los detalles generales de su configuración (Router -Gateway- y Servidor DNS). Si selecciona la interfaz de red (FastEthernet0) podrá observar la configuración IP de esta interfaz.

Una vez que esté familiarizado con el modelo de la red pase a la siguiente página.

[1] Los enlaces a ficheros de Packet Tracer están desactivados en el documento.

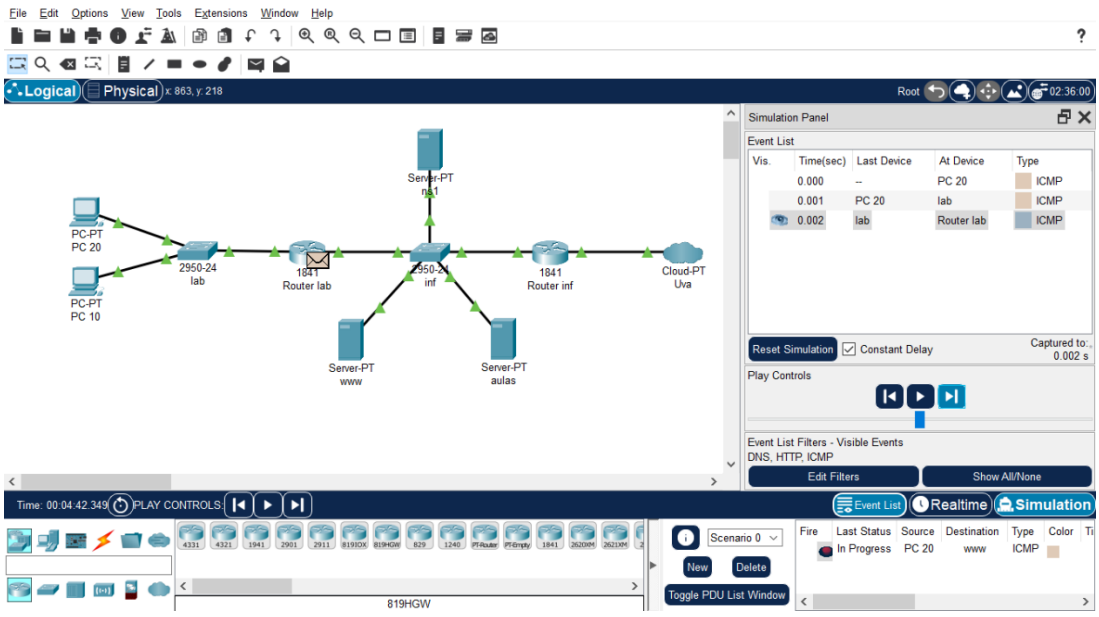
5.3 Comprobando la conectividad

Una vez cargado el modelo y familiarizado con el esquema de la red, vamos a comprobar que existe conectividad entre todos los elementos. Para ello vamos a hacer PINGs entre dos de ellos. Básicamente hay dos formas de conseguir esto:

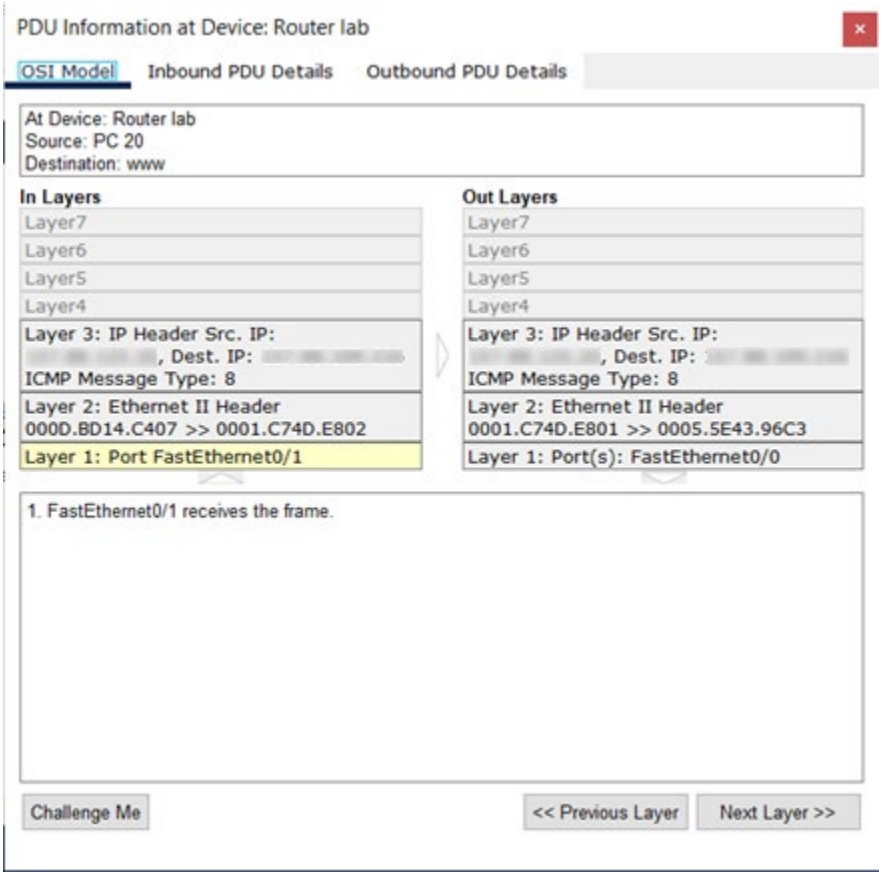
- picando en el dispositivo origen del ping, seleccionando **Desktop > Command Prompt**, lo que abre un intérprete de comandos similar al de Windows. Teclee el comando **ping <destino>** (donde <destino> es la dirección IP del destino).
- picando en el icono del menú  (**"Add simplePDU (P)"**), y después picando sobre el dispositivo origen y luego sobre el destino. El resultado del ping puede verse en el panel inferior derecho (éxito o fallo). En este mismo panel se puede repetir, editar o eliminar el ping, haciendo doble clic, respectivamente, en el icono/texto de la columna Fire, Edit o Delete de la fila correspondiente a nuestro ping.

Resulta interesante poder reproducir el ping paso a paso de modo que se pueda observar los paquetes que se generan y el camino que toman. Para ello seleccione el **modo Simulación** y edite el filtro para que sólo se muestren los paquetes ICMP. Realice un ping desde **PC20** a **PC10** y avance el tiempo paso a paso con el icono Capture/Forward  . Observe cómo el paquete viaja de PC20 a PC10 a través del switch.

Vuelva a realizar el ping desde **PC20** a la dirección IP del servidor www, pero esta vez utilizando la interfaz de comandos y avance el tiempo paso a paso. Observe cómo se generan y transmiten los paquetes por la red. Debería aparecer una ventana similar a la que aparece en la siguiente figura.



Si pica sobre uno de esos paquetes puede observar su contenido y el procesamiento que realiza el dispositivo con el paquete. Verá que hay dos o tres pestañas en la parte superior:



- **OSI Model:** Describe un resumen de las 7 capas del modelo OSI de ISO, y el procesamiento que realiza el dispositivo en cada capa. Si el paquete entrante genera un paquete saliente, habrá dos pilas de capas, una para el paquete entrante (In Layers) y otra para el saliente (Out Layers). Picando en cada capa, o bien picando en "Next Layer", puede verse el procesamiento que va haciendo el dispositivo y las decisiones que va tomando. Esto es muy útil para entender lo que ocurre cuando necesitamos investigar algún problema. Si hay capas en las que no aparece información es porque el dispositivo no procesa esas capas.
- **Inbound PDU Details:** Muestra el contenido del paquete entrante de forma similar a lo que hace Wireshark, pero con menos información.
- **Outbound PDU Details:** Esta pestaña aparecerá sólo si a consecuencia del paquete entrante se genera un paquete saliente (por ejemplo, porque el paquete entrante se reenvíe a otro dispositivo). Es similar a Inbound PDU Details, pero para el paquete saliente.

Juegue un poco con el ping en modo simulación y observe la información contenida en cada una de las capas de los protocolos que incorpora el paquete. Esto permite tener una visión parecida a la que obteníamos con la herramienta Wireshark, pero con paquetes simulados, no reales.

Una vez haya terminado de jugar, borre los pings que aparezcan en la ventana inferior derecha, y continue con el ejercicio.

Aquí se incluye una pregunta múltiple aleatoria de un banco de preguntas que requiere realizar un ping en packet tracer en modo simulación, ver por dónde pasa, y ver direcciones IP de interfaces y de default Gateway en PCs. Las preguntas múltiples son varias preguntas encadenadas.

5.4 Paquete ICMP en router y switch

En el modo simulación, repita el ping y presione Capture/Forward  hasta que el paquete ICMP llegue a "**Router inf**".

Abra el contenido de ese paquete pinchando sobre él. En la ventana emergente podemos visualizar la información que necesita procesar el dispositivo sobre el que está el paquete:

1. tanto del paquete que entra al Router (OSI Model -> IN layers --- capas de ENTRADA)
2. como del paquete que sale de este Router (OSI Model -> OUT layers --- capas de SALIDA).

Además podemos conocer más detalles y valores de los campos de cada capa en la pestaña **INbound PDU Details,** para el paquete de entrada, y **OUTbound PDU Details**, para el paquete de salida.

Aquí se incluye una pregunta múltiple aleatoria de un banco de preguntas que requiere abrir el contenido de un paquete de ping en modo simulación, ver las diferencias entre lo que procesa un router y un switch, y analizar la información que muestra packet tracer del contenido del paquete.

5.5 DNS

Ahora vamos a observar cómo se resuelven los nombres de dominio en DNS.

Active el modo simulación y añada el protocolo DNS al filtro de paquetes (de modo que ahora únicamente deberían estar activados los protocolos ICMP y DNS).

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren hacer un ping en el terminal de un PC usando el nombre de un destino en lugar de la

dirección IP, y analizar los paquetes DNS e ICMP que se generan, el camino que siguen, y su contenido.

5.6 Web

Borre los pings anteriores que haya en la ventana inferior derecha.

Ahora vamos a realizar una petición HTTP para acceder a la página web www.inf.uva.es.

Active el modo tiempo real.

Entre en el host PC20 y seleccione la utilidad **Web Browser** dentro de la pestaña **Desktop**.

En la caja de dirección escriba el nombre de host del servidor **www** y pique el botón **GO**.

Observará que se carga la página web correspondiente.

Realice ahora de nuevo la solicitud HTTP **en modo simulación**. Añada el protocolo HTTP a la lista de protocolos observados anteriormente (ICMP y DNS) y observe la secuencia de paquetes que se desarrollan identificando primero la resolución del nombre (DNS) y después la transacción web (HTTP).

Una vez que ha accedido a la página web del servidor www, pique en el enlace que aparece en ella para acceder a la web de **aulas**. Observe la secuencia de paquetes que se desencadena.

Aquí se incluye una pregunta aleatoria de un banco de preguntas que requiere abrir una página web desde un PC de packet tracer en modo simulación, y analizar los paquetes de los protocolos HTTP y DNS que se generan.

5.7 Servidor Web propio

Por último, vamos a crear nuestro propio "servidor HTTP" desde cero.

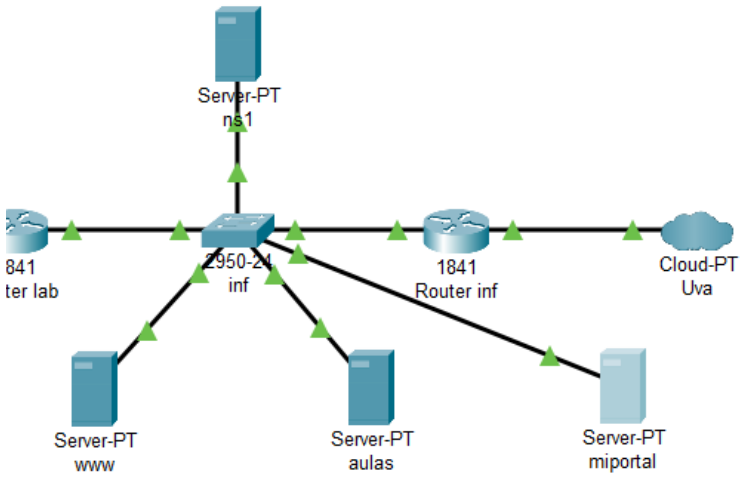
Seleccione el servidor www (para ello dibuje un recuadro alrededor del servidor mientras mantiene presionado el botón izquierdo del ratón).

Presione CTRL+C para copiarlo, y CTRL+V para pegarlo en el tapiz.

1. Pique sobre este servidor copiado, vaya a la pestaña **CONFIG->Settings**, y cambie el DisplayName por "miportal" o por otro nombre de su elección.
2. Cambie la dirección IP de la interfaz ethernet por una que no esté actualmente en uso dentro de la subred de los servidores, entrando en **CONFIG->INTERFACE->FastEthernet** y modificando el campo **IPv4 Address**. Cierre la ventana de configuración del PC.

3. Seleccione del panel de herramientas de abajo a la izquierda, el botón **CONNECTIONS (CONEXIONES)**, y seleccione el **Cable Directo (Copper Straight-Through).**

Pique sobre el servidor nuevo y seleccione una interfaz Ethernet y después sobre el switch de la derecha y seleccione también una de las interfaces Ethernet, para crear una conexión cableada (de igual modo que está el servidor www.inf.uva.es con el mismo switch).



Asegúrese de que está bien conectado y configurado verificando que las conexiones están en verde, y que funcionan los pings desde cualquier PC al servidor nuevo (puede ocurrir que fallen el primer y segundo ping, pero luego deberían funcionar).

Cuando lo haya comprobado, borre los pings anteriores que haya en la ventana inferior derecha.

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas para comprobar que se ha realizado lo que pide el guion, y que requieren registrar la traducción del nombre a IP del nuevo servidor en el servidor DNS.

6. HTTP y TCP

En esta práctica de laboratorio vamos a profundizar en el conocimiento y manejo de la herramienta Packet Tracer y mostrar cómo se puede analizar el comportamiento de los protocolos en las redes sobre una red simulada. En este caso, la ventaja que nos aporta una red simulada es que podemos acceder a la red tanto desde la perspectiva del cliente como del servidor. En otros casos utilizaremos esta herramienta para diseñar, configurar y probar redes completas.

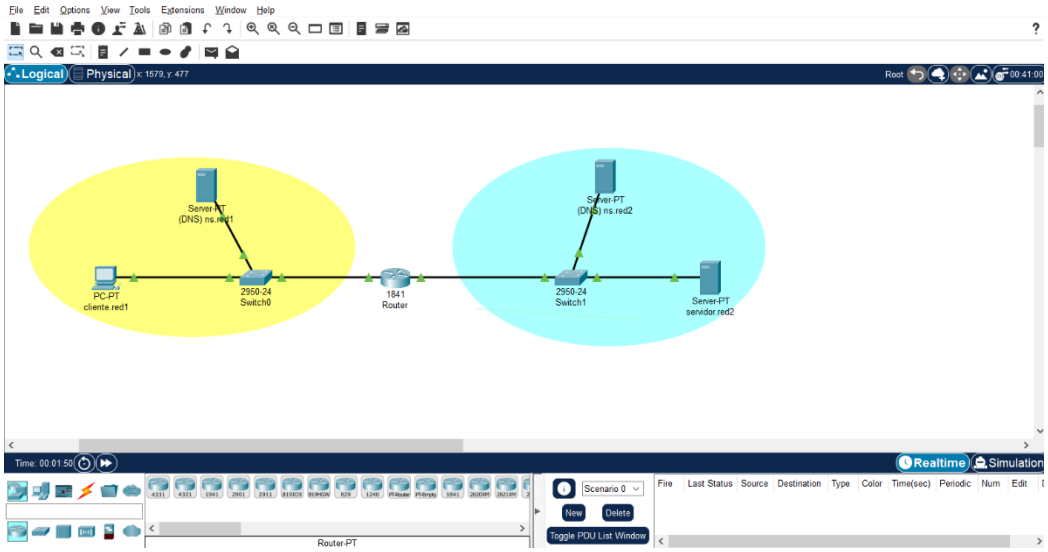
En este ejercicio nos vamos a centrar en el protocolo HTTP, que se asienta sobre TCP. También veremos cómo funciona DNS. Los objetivos de este ejercicio son los siguientes:

1. Analizar la naturaleza solicitud-respuesta de HTTP.
2. Comprender cómo se asienta HTTP sobre TCP.
3. Observar el intercambio de segmentos TCP y analizar los mecanismos de TCP implicados en la transferencia fiable de paquetes.
4. Observar cómo se resuelven consultas DNS sencillas previas a la realización de conexiones en la red.
5. Introducir en el manejo de la herramienta Packet Tracer.

6.1 Descripción de una pequeña red

Vamos a utilizar la herramienta que vimos en la sesión anterior para analizar el tráfico en una pequeña red ya configurada. Para comenzar siga los siguientes pasos: Descargue el archivo red.pkt[1], que es el que contiene la red sobre la que vamos a trabajar. Guarde el archivo donde pueda encontrarlo. Abra el programa Packet Tracer. Cargue el archivo anteriormente obtenido. Para ello ejecute la siguiente secuencia de opciones en el menu: **File > Open** y elija el archivo red.pkt Debería aparecer la siguiente ventana:

[1] Los enlaces a ficheros de Packet Tracer están desactivados en el documento.



La red tardará unos instantes en estabilizarse, lo que se puede percibir porque los puntos que representan las interfaces de red son de color verde. Dé tiempo a que todos los elementos de la red se activen y carguen las configuraciones **(puede presionar el botón "Fast Forward Time" para acelerar este proceso).**

6.2 Presentación de la Red

La red sobre la que vamos a trabajar consiste en dos redes conectadas por un router. En la red de la izquierda, la zona amarilla, se encuentra un host que va a jugar el papel de cliente. El servidor está en un host de la red de la derecha (zona azul). En ambas redes existe un servidor de nombres DNS (ns). Los elementos que restan de describir son switches, switch0 y switch1, y por ser dispositivos de la capa 2, no vamos a prestarles más atención en este momento y sólo diremos que son necesarios para conectar todos los elementos.

6.3 REPASO de la herramienta Packet Tracer: zonas, información y funcionalidades.

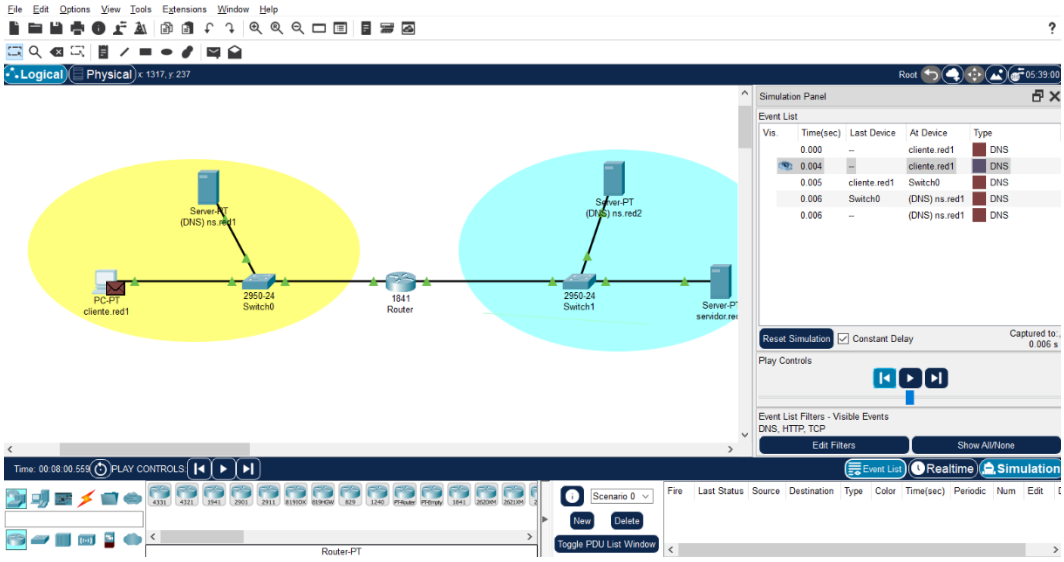
La herramienta Packet Tracer es un software que nos permite diseñar redes (cables, host, etc.), configurar los distintos elementos (dir. IP, servidores HTTP, DNS, etc.) y simular su funcionamiento (traza paso a paso, análisis de paquetes, etc.).

Para diseñar (dibujar) una red se utilizan los elementos en la paleta que figura en la parte inferior de la ventana. Una vez declarados los elementos que van a formar la red, se configuran a partir de la ventana que aparece tras hacer click en ellos.

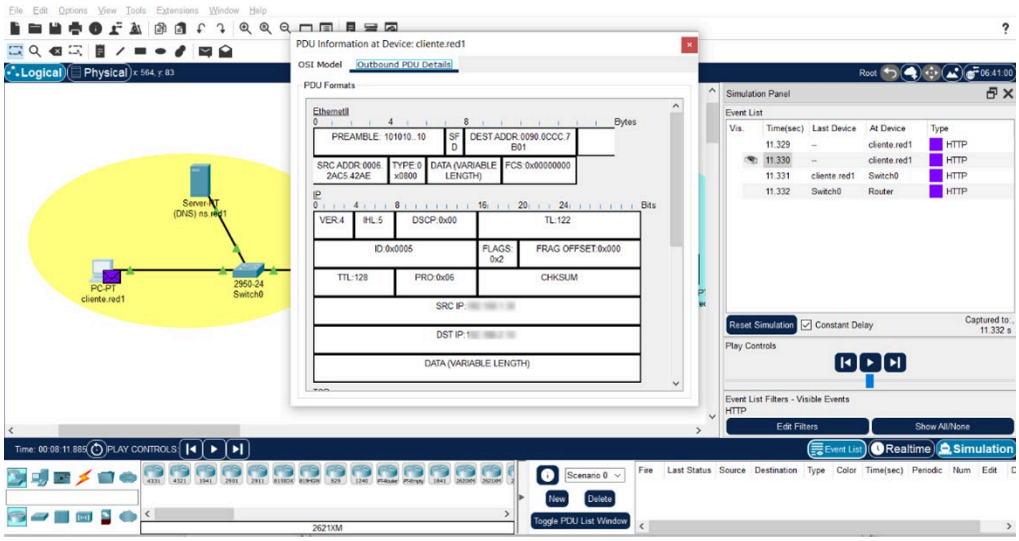
En este caso se trata de observar una red ya diseñada y configurada, por lo que no vamos a utilizar estas posibilidades de diseño y configuración. La capacidad de prueba y simulación de Packet Tracer es la más interesante, y será sobre la que vamos a trabajar en este caso.

Los distintos hosts presentes pueden utilizar los protocolos de red pues incorporan aplicaciones como acceso al terminal, cliente web, y otras. Para ello, debemos picar en el elemento deseado, e ir a la pestaña **Desktop**. Allí se encuentran distintas aplicaciones disponibles: Telnet, navegador Web, etc.

Una vez desencadenada una operación en la red, podemos analizar su resultado en dos modos: Tiempo Real o Simulación. En el modo Tiempo Real (**Real Time**), las operaciones se muestran en la parte inferior derecha de la ventana, junto con los datos que permiten identificar si fueron exitosas o no, así como otros detalles sobre su desarrollo. En el modo Simulación (**Simulation**) se puede observar el paso de los paquetes por la red, bien paso a paso (**Capture/Forward**) o de modo automático (**Auto Capture/Play**). Los distintos tipos de paquetes se van mostrando asociados a un color. Se puede elegir los protocolos deseados, filtrando el resto e impidiendo que aparezcan así en la simulación. Esto se puede hacer en el botón **Edit Filters**.



Los paquetes se pueden analizar con detalle, ya que Packet Tracer nos muestra el contenido de los mismos en las distintas capas TCP/IP (ISO OSI). Para ello, una vez seleccionado un paquete, picando sobre él, se abre una ventana en la que se muestra la pila de protocolos y los valores de las tramas de las distintas capas. Con los botones **Previous Layer** y **Next Layer** se puede navegar por las distintas capas, lo que permite observar el contenido de los paquetes y recibir una explicación de su contenido. Con ello podemos ver el procesamiento que realiza el dispositivo en cada una de las capas de la pila TCP/IP.



Ahora que ya se han presentado las posibilidades de Packet Tracer en general, aproveche un momento para investigar sobre las mismas si es que no lo ha hecho ya durante las explicaciones anteriores. Resulta imprescindible que se familiarice con sus posibilidades y su manejo ya que será necesario su manejo en el resto del ejercicio, así como en las siguientes prácticas y en los proyectos de la asignatura.

Cuando haya experimentado y curioseado lo suficiente avance al siguiente paso del ejercicio.

6.4 Mensajes HTTP

En este primer caso, vamos a analizar el intercambio de mensajes HTTP. La aplicación Packet Tracer debe estar en funcionamiento con la red de ejemplo (archivo red.pkt) cargada. Si sospecha que en el paso anterior haya podido modificar la red de algún modo, vuelva a cargar el archivo de nuevo descartando los cambios realizados.

Realice las siguientes acciones:

1. Coloque la herramienta en modo simulación picando en el botón **Simulation** que aparece en la parte inferior derecha de la ventana.
2. Vamos a indicar que sólo deseamos ver los paquetes HTTP. Para ello en la ventana que aparece picando en **Edit Filters**, realice las operaciones necesarias para que únicamente HTTP permanezca seleccionado y cierre la ventana de filtros.
3. Inicie una solicitud HTTP desde el cliente. Para ello, pique sobre el host cliente, y en la pestaña **Desktop**, seleccione **Web Browser**. Entonces aparecerá un navegador web mínimo. En la caja de dirección URL introduzca la dirección IP del servidor y pulse en **Go**.
4. Inicie la simulación avanzando sólo un paso, picando en el

botón **Capture/Forward**  una sola vez. Si el proceso avanza más allá de forma involuntaria, se puede volver atrás con el botón **Back**.

Seleccione el paquete HTTP que ha generado el cliente, y observando su información responda a las preguntas que se realizarán a continuación.

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren analizar con packet tracer en modo simulación el contenido de paquetes HTTP.

6.5 Solicitud HTTP llega al servidor

Con el botón **Capture/Forward**  haga avanzar el paquete con la solicitud HTTP hasta que llegue al servidor, contando el número de saltos que componen el trayecto. Si picamos con el ratón el paquete para observar su contenido, podemos ver que presenta 2 pilas paralelas, una de entrada a la izquierda (**In Layers**) (paquete entrante, en este caso la petición HTTP que llega) y otra de salida a la derecha (**Out Layers**) (paquete saliente, en este caso la respuesta HTTP que envía el servidor). Con los datos de ese paquete en la ventana, responda a las siguientes preguntas.

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren analizar con packet tracer en modo simulación el contenido de paquetes HTTP.

6.6 Recepción respuesta HTTP

Permita que la simulación continúe (mejor paso a paso) hasta que el paquete con la respuesta HTTP alcance el cliente que realizó la solicitud. Picando en el cliente, compruebe que el navegador web muestra la página solicitada. Seleccione el paquete recibido en el cliente y con el visor de información del mismo en la capa 4 responda a las siguientes preguntas.

Aquí se incluye una pregunta aleatoria de un banco de preguntas que requiere analizar con packet tracer en modo simulación el contenido de paquetes HTTP.

6.7 TCP entra en escena

Ahora vamos a analizar el modo en que TCP transporta los mensajes HTTP. Para ello, sin necesidad de realizar otra simulación, vamos a incluir el protocolo TCP en el filtrado de paquetes:

1. Localice y pique el botón "**Edit Filters**".
2. En la ventana que surge, seleccione el protocolo TCP que podrá encontrar en la etiqueta "Misc".
3. Cierre la ventana de filtro. Ahora podrá ver los paquetes TCP y HTTP.

Ahora podrá observar que han aparecido muchos más paquetes en la ventana de eventos de la simulación (derecha). Con los botones "**Back**" y "**Capture/Forward**" lleve la simulación al inicio, y después hasta el momento en que el primer segmento TCP alcanza el servidor. Pique sobre el paquete para ver su contenido y conteste a las siguientes preguntas:

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren analizar con packet tracer en modo simulación el contenido de paquetes TCP.

6.8 DNS a escena

Ahora vamos a analizar el papel que juega la resolución de nombres en la red, y en concreto en la solicitud HTTP. Para poder verlo, será necesario que active DNS en la lista de protocolos del filtro ("**Edit Filters**") que se encuentra bajo la etiqueta "IPv4".

Investigue un poco por su cuenta sobre la diferencia de comportamiento entre realizar la petición HTTP desde el navegador web del host cliente utilizando la dirección IP del servidor y hacerlo utilizando su nombre: "**servidor.red2**".

Tiene que tener en cuenta que para saber si un DNS resuelve una consulta DNS, tiene que picar en el paquete entrante en el DNS y observar lo que le indica la capa DNS de '*In Layers*'.

Para borrar los paquetes de la consulta anterior y que no se confundan con las nuevas operaciones a realizar en la red, puede picar en el botón "**Delete**" Delete de la parte inferior, o en el botón "**Reset Simulation**" Reset Simulation que le aparece en la ventana en modo simulación.

Una vez haya jugado un poco, antes de continuar tiene que borrar la caché de DNS del servidor DNS de la red 1 (izquierda). Para ello, seleccione el servidor de la red1, y pique la siguiente secuencia de opciones:"**Services > DNS > DNS Cache > Clear Cache**".

Realice de nuevo la petición http desde el host cliente.red1, utilizando el nombre del servidor servidor.red2 en lugar de su dirección IP y conteste a la siguiente pregunta.

Aquí se incluye una pregunta aleatoria de un banco de preguntas que requieren analizar con packet tracer el funcionamiento del protocolo DNS y el contenido de sus paquetes.

Vamos a realizar otra consulta DNS sobre el mismo dominio de antes: **servidor.red2**. Para ello,

1. Reinicie la simulación picando el botón "**Reset Simulation**".
2. Vuelva a realizar una petición HTTP desde el navegador web del cliente indicando "**servidor.red2**" como URL deseada.
3. Avance la simulación y observe quién resuelve la consulta en esta ocasión
4. Lleve la simulación hasta el punto en que un servidor DNS resuelve su consulta DNS y responda a las siguientes preguntas.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas que requieren analizar con packet tracer el funcionamiento del protocolo DNS y el contenido de sus paquetes.

Observe la configuración DNS de **ns.red1**. Para ello siga los siguientes pasos:

1. Pique sobre "**ns.red1**".
2. En la pestaña "**Services**", seleccione "**DNS**" para observar la configuración del DNS (el contenido de su base de datos).
3. Pique "**DNS Cache**" para observar el contenido de la caché (debería aparecer una entrada correspondiente a "**servidor.red2**" a la que se hizo referencia en la consulta anterior).
4. Cierre la ventana de la caché (**Cancel**).
5. Observe la base de datos DNS (los *"resource records"* que hay configurados)

> Aquí se incluye una pregunta aleatoria de un banco de preguntas que requieren analizar con packet tracer el funcionamiento del protocolo DNS y el contenido de sus paquetes.

> Aquí se incluye una pregunta final de autorreflexión y síntesis sobre la práctica realizada y los conocimientos adquiridos.

7. Asignación estática y dinámica de direcciones IP

7.1 Introducción y Objetivos

En esta práctica de laboratorio, usted aprenderá y utilizará los aspectos fundamentales del direccionamiento IP. En concreto, los objetivos de este ejercicio son los siguientes:

- Describir las características y el uso del direccionamiento IP
- Identificar la dirección IP y la máscara de subred
- Determinar cuál de las partes de una dirección IP es el ID de red y cuál es el ID de host
- Identificar las direcciones IP de host válidas y no válidas basándose en las normas de direccionamiento IP
- Definir el rango de direcciones y máscaras de subred
- Comprender y distinguir los modos de asignación de direcciones estático y dinámico (DHCP)

7.2 Información Básica

Esta práctica de laboratorio le ayudará a ampliar su comprensión acerca de las direcciones IP y de la forma en que operan las redes TCP/IP. Es en primer lugar un ejercicio de práctica de laboratorio escrito, para posteriormente convertirse en un ejercicio sobre Packet Tracer.

Sin embargo, sería conveniente revisar algunas direcciones IP de red reales utilizando las utilidades de línea de comando **ipconfig** para Windows NT/2000/XP o **/usr/sbin/ifconfig** para Linux.

Las direcciones IP se utilizan únicamente para identificar redes y hosts TCP/IP individuales como, por ejemplo, computadoras e impresoras en red de manera que los dispositivos se puedan comunicar entre sí. Las estaciones de trabajo y los servidores en una red TCP/IP se denominan hosts, que se conectan a la red mediante una interfaz de red, y cada interfaz posee una dirección IP única. Esta dirección se conoce como dirección de host.

Para que un host pueda acceder a Internet, debe tener una dirección IP. En su forma básica, la dirección IP consta de dos partes:

- Un identificador de red

- Un identificador de host

La Corporación de Internet para la Asignación de Nombres y Números (ICANN), a través de los Registros Regionales de Internet (RIR), por ejemplo, RIPE en Europa, asigna la parte de red de la dirección IP a una empresa u organización, y luego es esta organización la que asigna la dirección del host dentro de su subred a cada uno de los hosts conectados (o mejor dicho a sus interfaces de red).

Los **routers** usan la dirección IP para encaminar paquetes de datos entre redes. Las direcciones IP tienen una longitud de 32 bits, de acuerdo con la versión IPv4, y se dividen en 4 octetos (bytes) de 8 bits cada uno. Operan en la capa de red (Capa 3) del modelo TCP/IP.

Las direcciones IP se asignan de la siguiente manera:

- De manera estática: manualmente, a través de un administrador de red
- De manera dinámica: automáticamente, a través de un servidor de Protocolo de Configuración de Host Dinámico (DHCP: Dynamic Host Configuration Protocol)

La dirección IP de una estación de trabajo o host es una dirección lógica, lo que significa que se puede modificar. La interfaz de red tiene asignada otra dirección denominada de dirección de Control de Acceso al Medio o MAC (MAC: Media Access Control) que es una dirección de 48 bits que en principio no se puede alterar. Esta dirección se graba en la tarjeta de interfaz de red (NIC) y no se puede cambiar a menos que la NIC sea reemplazada. Por ello se suele denominar dirección física. La MAC es usada principalmente en la capa de enlace, mientras que en la capa de red (IP) se usa la dirección IP.

La combinación de la dirección IP lógica y de la dirección MAC física ayuda a encaminar los datagramas hacia el destino correcto.

En las direcciones IP hay una parte de la dirección que corresponde a la red y otra parte al host. En esta práctica de laboratorio, se trabajará con diferentes direcciones IP para ayudar a familiarizarse con las características de cada una de ellas. La comprensión de las direcciones IP es fundamental para comprender TCP/IP y las interconexiones de redes en general.

7.3 Revisión del direccionamiento IP y sus características

Una **dirección IP** es una dirección utilizada para identificar de forma única un dispositivo en una red IP. La dirección se compone de 32 bits, que pueden dividirse en una parte de red y una parte de host con la ayuda de una **máscara de subred**.

Los 32 bits se dividen en cuatro octetos (1 octeto = 8 bits). Cada octeto se convierte a decimal y se separa por un punto. Por este motivo, se dice que una dirección IP se expresa en formato decimal con notación punto (por ejemplo, 172.16.81.100). El valor en cada octeto varía entre 0 y 255 en decimal o 00000000 - 11111111 en binario.

Tradicionalmente, las direcciones IP públicas se asignaban en función de los límites de clase:

- Clase A: rango de direcciones 1.0.0.0 a 126.0.0.0, número de hosts $2^{24} - 2$ = 16,777,214, máscara 255.0.0.0
- Clase B: rango de direcciones 128.0.0.0 a 191.255.0.0, número de hosts $2^{16} - 2$ = 65,534, máscara 255.255.0.0
- Clase C: rango de direcciones 192.0.0.0 a 223.255.255.0, número de hosts $2^{8} - 2$ = 254, máscara 255.255.255.0
- Clase D: rango de direcciones 224.0.0.0 a 239.255.255.255, para multicast
- Clase E: rango de direcciones 240.0.0.0 a 255.255.255.255, reservada (formalmente experimental)

En 1993 se presentó el CIDR (Classless inter-domain routing) por Internet Engineering Task Force con los siguientes objetivos:

1. hacer frente al problema de agotamiento de direcciones IPv4
2. ralentizar el crecimiento de las tablas de enrutamiento

CIDR usa máscaras de subred de longitud variable (VLSM - *Variable Length Subnet Mask*) para asignar direcciones IP a subredes de acuerdo con la necesidad individual en lugar de hacerlo por la clase.

7.3.1 Máscara de subred

El CIDR se basa en el concepto de las **máscaras de subred**. Una máscara se superpone a una dirección IP y señala qué parte de la dirección IP se reserva a los hosts (a cada integrante de la red) y qué parte identifica a la red.

Una máscara de subred es un número de 32 bits donde los bits a 1 indican la parte de la red y los bits a 0 indican la parte del host. Los sistemas informáticos determinan qué parte es red y qué parte es host realizando un AND lógico. Si tenemos:

- Dirección IP: 10.0.1.1 = 00001010.00000000.00000001.00000001
- Máscara de subred: 255.0.0.0 = 11111111.00000000.00000000.0000000

El identificador de la red será 10.0.0.0 = 00001010.00000000.00000000.00000000

Una máscara de subred siempre debe ser una serie de unos (1) seguida de una serie de ceros (0).

Además del formato decimal con puntos, también podemos escribir la máscara de subred en notación prefijo con barra inclinada '/' seguida del número de bits de la máscara de subred. Por ejemplo, tenemos la máscara de subred 255.0.0.0. En binario, es 11111111.00000000.00000000.0000000. El número de 1 consecutivos es 8, por lo que la notación prefijo será /8.

7.3.2 Dirección de red y de host

La parte de la dirección que corresponde a la red o al host no puede estar formada exclusivamente por unos o por ceros. Como ejemplo, la dirección 118.0.0.5/8 es una dirección IP válida. La porción de red o los primeros 8 bits, que equivalen a 118, no consta sólo de ceros y la porción de host o los últimos 24 bits, no consta de todos ceros o unos.

Si la parte que corresponde al host estuviera constituida exclusivamente por ceros, ésta sería la dirección de la propia red (significaría "*esta red*").

Si la porción de host fuera igual a todos unos, sería un *broadcast* para la dirección de red (significaría "*todos los hosts de esta red*").

El valor de cualquiera de los octetos nunca puede ser superior al 255 decimal o al 11111111 binario.

Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre máscaras de subred

7.3.3 Direcciones especiales

Algunos rangos de direcciones IP son especiales, y están reservadas para usos concretos y no se pueden asignar a hosts:

- El dispositivo de red loopback es una interfaz de red virtual que suele hacer referencia al propio dispositivo, y por lo tanto suele usarse cuando se envían paquetes al propio dispositivo. Las direcciones del rango **127.0.0.0/8** son direcciones de loopback, de las cuales se utiliza, de forma mayoritaria, la **127.0.0.1** por ser la primera. Se usa en un host para comprobar que la configuración TCP/IP funciona correctamente.
- El rango 224.0.0.0 al 239.255.255.255 está reservado para multicast.
- El rango 240.0.0.0 al 254.255.255.255 está reservado para uso experimental en investigación.

7.3.4 Direcciones públicas y privadas

Las direcciones IP son en general públicas y no puede haber dos dispositivos en Internet con la misma IP.

Las direcciones privadas se incorporaron en los 90s (RFC 1918) debido al agotamiento de las direcciones IPv4.

Son direcciones no enrutables en internet (necesitan ser convertidas a una dirección IP pública para acceder a internet: NAT)

Se usan sólo para redes internas

La ventaja que tiene usar direccionamiento privado internamente es que se ahorran direcciones públicas.

Los siguientes rangos de direcciones IP son bloques de direcciones privadas:

- **10.0.0.0/8** : de 10.0.0.0 a 10.255.255.255 --> Se suele usar para definir subredes /8
- **172.16.0.0/12** : de 172.16.0.0 a 172.31.255.255 --> Se suele usar para definir subredes /16
- **192.168.0.0/16** : de 192.168.0.0 a 192.168.255.255 --> Se suele usar para definir subredes /24

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas sobre direccionamiento IP

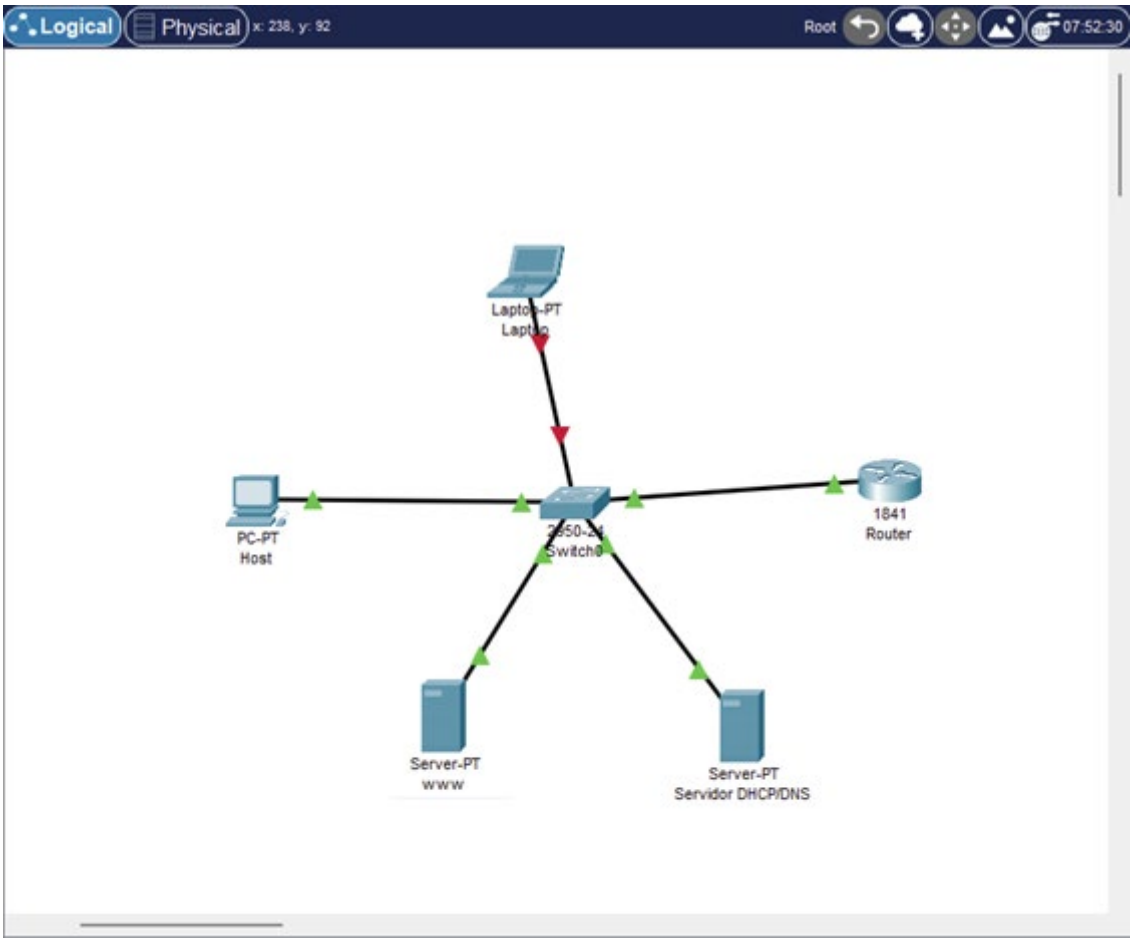
7.4 DHCP

Ahora simularemos el comportamiento de una red sencilla con asignación dinámica de IP a través del protocolo DHCP utilizando Packet Tracer.

Arranque el programa Packet Tracer y cargue la red del archivo pkt[1].

La red se puede observar en la siguiente figura.

[1] Los enlaces a ficheros de Packet Tracer están desactivados en el documento.



Dicha red consta de un router, un servidor DHCP/DNS (el servicio DNS está desactivado), un servidor web, un host y un portátil.

Indague por su cuenta en los detalles sobre la red. Observe que el portátil se encuentra con la interfaz de red desactivada, lo que equivale a encontrarse desconectado de la red. Por ello los pilotos se muestran en color rojo. Deje que por ahora permanezca de este modo.

Espere a que los enlaces se estabilicen (piloto verde) y entonces realice una petición http desde el host a la dirección IP del servidor www (ya debería saber cómo realizarlo: con el navegador de internet en el host y poniendo como URL la dirección IP). Observe la respuesta obtenida.

Con la red cargada, realice las operaciones que se le indican en la siguiente página y responda a las consultas que vienen a continuación.

Ahora vamos a proceder a conectar la interfaz de red de laptop. Para ello pique sobre el icono de laptop > config > Fast Ethernet0 y active la casilla Port Status (ON).

Acelere, si es necesario, el tiempo mediante la pulsación del botón FastForward hasta que la conexión asociada al switch desde dicho laptop pase a estado verde.

Coloque el simulador en modo simulación (seleccione cronómetro en la zona inferior derecha).

Filtre los protocolos que nos interesan para analizar la transacción. En este caso active DHCP si no lo está ya y desactive el resto.

Ahora vamos a activar la configuración IP dinámica de laptop, así que en la misma ventana de configuración de laptop anterior (Fast Ethernet), active la casilla DHCP en 'IP Configuration'.

> Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren analizar con packet tracer en modo simulación el funcionamiento del protocolo DHCP, el contenido de sus paquetes, y el direccionamiento IP de los dispositivos implicados.

> Aquí se incluye una pregunta final de autorreflexión y síntesis sobre la práctica realizada y los conocimientos adquiridos.

8. Encaminamiento por defecto, estático y dinámico

8.1 Introducción y Objetivos

En este ejercicio de laboratorio, se pretende profundizar en el conocimiento del mecanismo y protocolos de encaminamiento en redes a partir de la realización de diversas configuraciones de red con el Packet Tracer. Al final de este ejercicio se habrán mejorado las destrezas en la configuración de routers en redes sencillas.

Los objetivos de esta lección son:

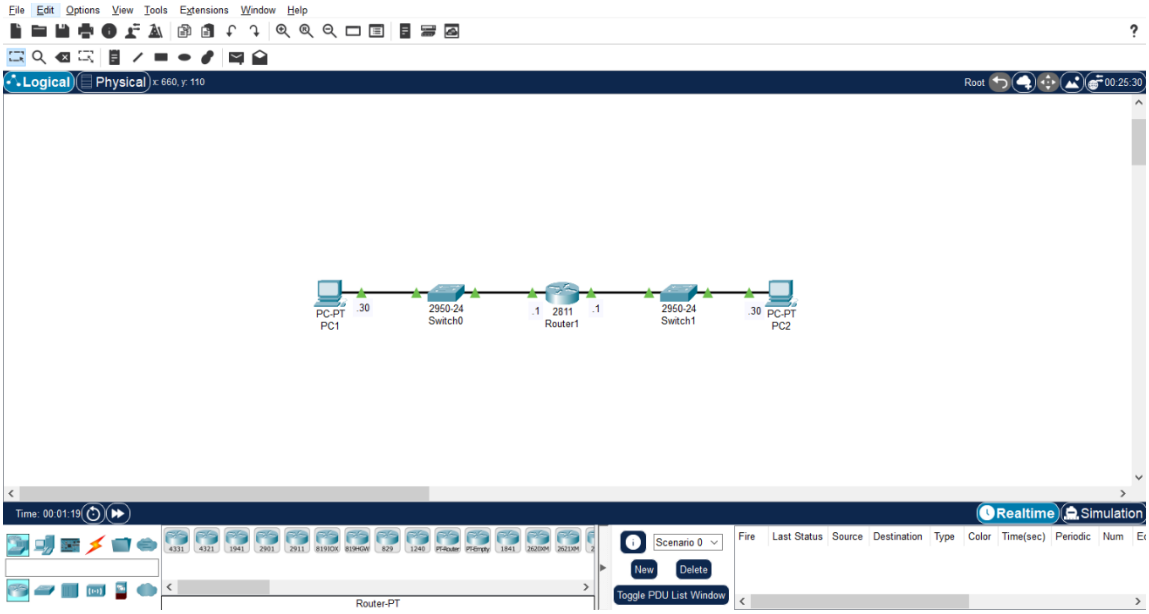
- Diseñar esquemas de direccionamiento para redes sencillas.
- Diseñar estrategias de encaminamiento estático y dinámico en redes sencillas y configurar los routers de acuerdo con ellas.
- Aprender a diseñar, construir, configurar y operar redes sencillas en Packet Tracer.

8.2 Caso 1: 2 subredes y 1 router

En este primer paso vamos a estudiar cómo se configura el encaminamiento de una LAN compuesta por dos subredes y un router que las interconecta.

Descargue el archivo red1router.pkt[1] y ábralo con el programa Packet Tracer. Debería aparecer una red como la de la siguiente figura.

[1] Los enlaces a ficheros de Packet Tracer están desactivados en el documento.

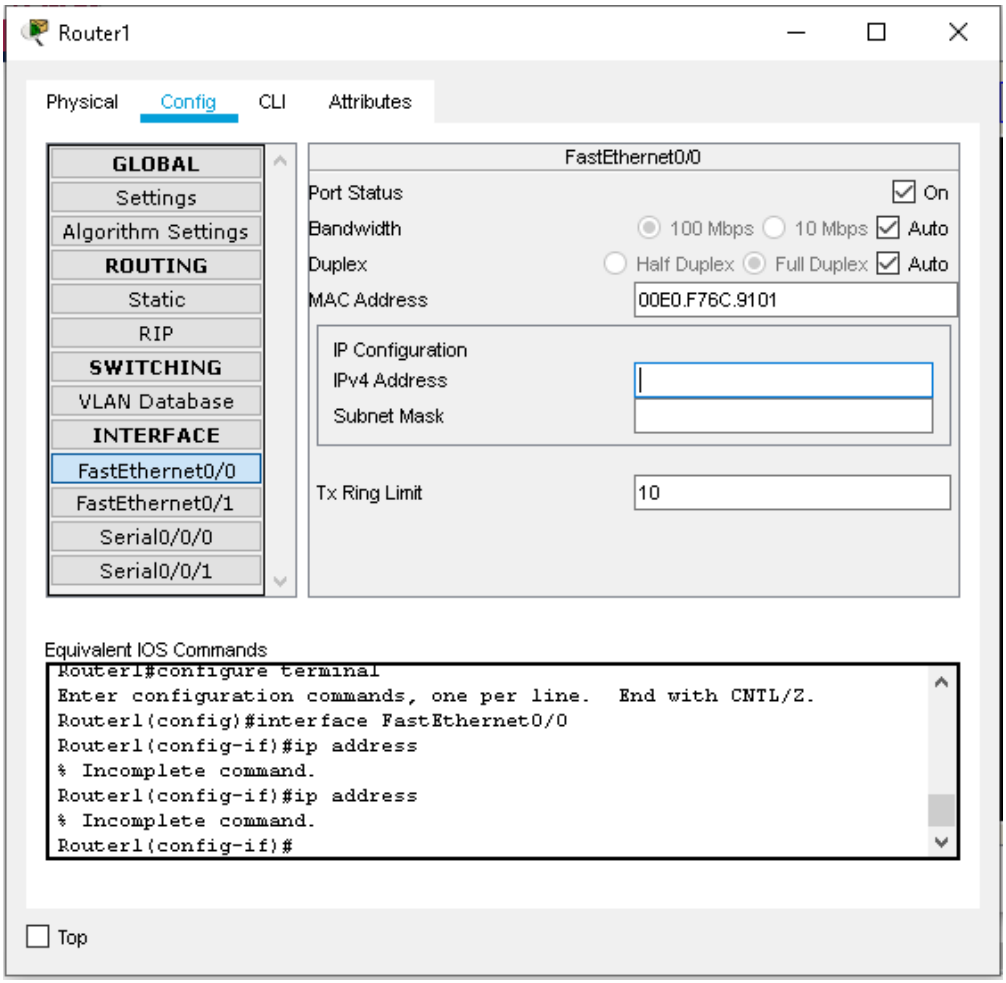


Observe las distintas configuraciones IP de las dos subredes, y compruebe mediante un ping entre PC1 y PC2 que la red no funciona. Los paquetes consiguen llegar al router, pero no consiguen atravesarlo. La razón es que aunque los host tienen bien configurado su router por defecto, Router1, éste no tiene configuradas sus interfaces, y por lo tanto el host PC1 no encuentra la interfaz de red de su router por defecto a la que entregar el paquete saliente.

En este caso, el encaminamiento resulta muy sencillo, pues la LAN está compuesta sólo por dos subredes conectadas por un router con interfaces conectadas a cada una de ellas. Así que el router será capaz de traspasar paquetes entre ambas subredes. Esta información de encaminamiento la obtiene el router a partir de las subredes a las que pertenecen las direcciones IP de sus interfaces.

Configure las direcciones IP y máscaras de las interfaces de red del router.

Para los detalles concretos de cómo hacerlo puede servirse de la siguiente figura donde se muestra la ventana donde se deben indicar la dirección (IPv4 Address) y la máscara (Subnet Mask) para cada interfaz (FastEthernet0/0 en este caso, igual para FastEthernet0/1):



Consejo: después de cualquier modificación en la configuración del router guárdela para que perdure: **Config > Settings > Save**.

La información de la tabla de reenvío se nutre en este caso de manera automática de la información que extrae de las direcciones asignadas a las interfaces de red y como no hay más subredes no conectadas directamente al router1, es suficiente para saber encaminar cualquier paquete ya que el router está conectado directamente a las dos únicas subredes existentes.

Compruebe ahora que la red funciona y el ping entre PC1 y PC2 se realiza con éxito. Puede que necesite un par de pings para que funcione, ya que, aunque esté todo bien configurado, puede que el router descarte el primer paquete que le llegue. En caso de que la red no funcione, compruebe los siguientes elementos por este orden:

1. **Existe conectividad física**: las interfaces están en verde y activas (situando el ratón

sobre el equipo, Link = up) y conectadas a los puertos en los que han de estar conectados. Los enlaces serie tienen señal de sincronización.

2. **Existe conectividad en el nivel de red**: las interfaces de hosts y routers tienen la dirección IP y la máscara y todas son correctas; los hosts tienen configurado el router por defecto, también llamado gateway por defecto o sencillamente gateway (se ve poniendo el cursor encima del router, o picando en el router y 'Config > Settings'); los paquetes llegan hasta el gateway por defecto; los paquetes con origen y destino en diferentes subredes llegan hasta el router y lo atraviesan.

Una vez que la red funcione, avance a la siguiente página.

8.3 Tabla de encaminamiento

La **tabla de enrutamiento** o de encaminamiento, o sencillamente tabla de rutas, es una tabla que contiene la información de las distintas rutas a los posibles destinos de una red. Cualquier equipo que tiene interfaces IP, y que por lo tanto procesa la capa IP, suele tener una tabla de encaminamiento. Esta tabla define por qué interfaz se envían los paquetes que le llegan al dispositivo. Además de la interfaz, si el paquete es dirigido a una red que no está directamente conectada, la tabla de encaminamiento contiene también la información del **gateway**, siguiente router, o siguiente salto (**next hop**) a quien tiene que dirigir el paquete para dicha ruta. Cada ruta tiene asociada también una **métrica**, que sirve para priorizar unas rutas sobre otras en caso de que haya varias rutas a un mismo destino.

Un ejemplo de una tabla de rutas con una única ruta sería el siguiente (la forma en que se representa la información depende del dispositivo y proveedor):

Network destination	Netmask	Gateway	Interface	Metric
192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.2	1

Tanto hosts como routers tienen tablas de rutas, ya que ambos procesan la capa IP. Los switches, por otro lado, no tienen tabla de rutas, ya que éstos no procesan la capa de red, sólo las capas 1 y 2.

La tabla de rutas se rellena automáticamente con la información de las redes directamente conectadas, las rutas configuradas a mano (rutas estáticas), y las rutas aprendidas dinámicamente de otros routers, en caso de que se use un protocolo dinámico de encaminamiento.

Es interesante que aprenda a ver la tabla de rutas en los distintos dispositivos de una red. Por ejemplo, **pruebe a ver la tabla de rutas de su PC o portátil** abriendo un terminal y ejecutando el comando:

```
netstat -rn
```

(la opción n sirve para que las redes le aparezcan en formato numérico y el dispositivo no resuelva el nombre).

Una vez visto lo anterior, **conéctese a una máquina linux**, y ejecute los siguientes comandos:

```
netstat -rn
route -n
```

Verá que el resultado con ambos comandos es similar, pero no exactamente el mismo.

En **Packet Tracer** también podemos ver la tabla de rutas de los distintos dispositivos. Por ejemplo, en la red con la que está trabajando en esta práctica, **pique en cualquier PC** y en 'Desktop > Command Prompt' ejecute el comando

```
netstat -r
```

Para ver la tabla de encaminamiento **en un router** hay que acceder a la consola de comandos (**CLI**) del router (picando en el router, CLI).

Dentro del CLI, hay básicamente tres modos de funcionamiento:

- Modo normal: se indica con un ">" en el prompt. Sirve para ejecutar comandos básicos para ver el estado del router.
- Modo privilegiado, supervisor, o enabled: se indica con un "#" en el prompt. Permite realizar comandos avanzados, reiniciar el router y acceder a la configuración. Se accede a él con el comando '**enable**' desde el modo normal.
- Modo configuración: se indica con "(config)" en el prompt. Se accede a él desde el modo privilegiado y permite configurar el router. Dentro del modo configuración hay una jerarquía de niveles de configuración, en los que se va entrando uno a uno. Para ir hacia atrás un nivel en la jerarquía se utiliza el comando **exit** (se sale del nivel actual). Se puede salir de todos los niveles pulsando **control + z**.

En Packet Tracer, cuando se accede al CLI, éste estará en el último nivel que se haya usado, aunque se haya hecho en modo gráfico. Si hemos configurado algo en modo gráfico, Packet Tracer, internamente, habrá ido al nivel correspondiente en el CLI y habrá ejecutado los comandos necesarios, de forma transparente al usuario. Por ello, al entrar en el CLI, conviene empezar siempre desde el estado inicial pulsando **control + z**.

Pique en el router, entre en el CLI, y en modo privilegiado ejecute el siguiente comando para ver la tabla de rutas:

```
show ip route
```

En la primera columna se indica con un código cómo se ha aprendido dicha ruta. Los códigos están explicados en la parte superior de la salida del comando.

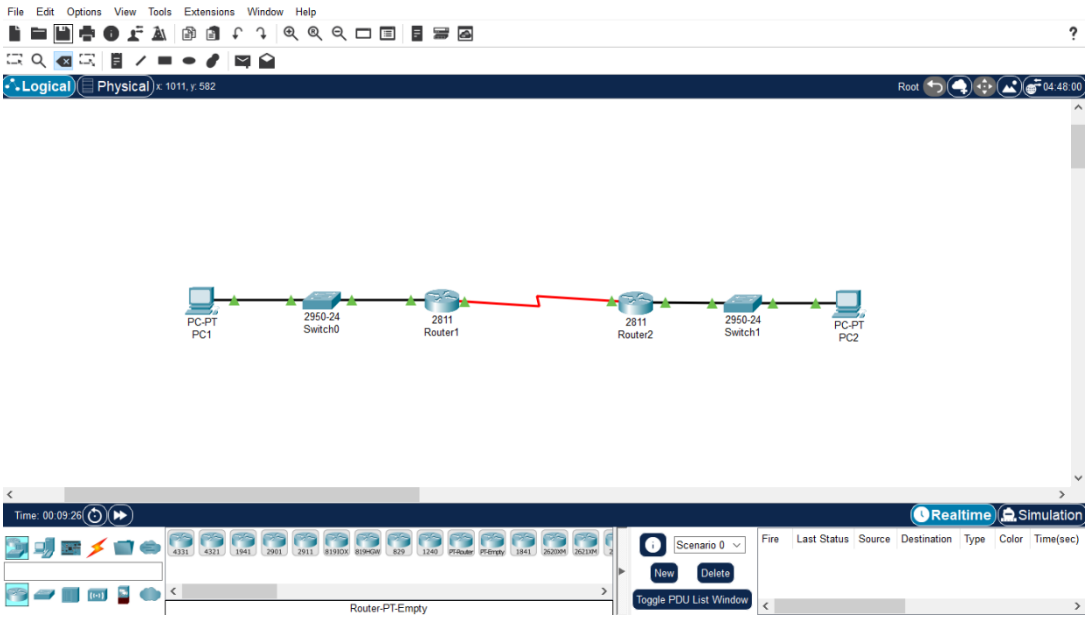
Una vez haya realizado con éxito los pasos anteriores responda a la siguiente pregunta.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas que requiere conectarse a una máquina Linux por ssh y obtener y entender su tabla de encaminamiento.

8.4 Caso 2: 3 subredes y 2 routers

En el siguiente paso, se va a modificar un poco la red de partida, añadiendo un segundo router. Ahora las dos subredes ya conocidas tendrán cada una un router por defecto distinto, y se necesitará una subred más para permitir la comunicación entre los dos routers.

Realice las operaciones necesarias para conseguir una configuración de este escenario, tal y como aparece en la figura siguiente y se explica a continuación.



Añadir un router: La opción más sencilla para añadir el nuevo router es copiar y pegar el que ya existe, obteniendo una copia. Seleccione el router pinchando y arrastrando alrededor de él. Utilice Ctrl+C para copiar y Ctrl+V para pegar la copia en el tapiz.

Si prefiere añadir un router usando el menú inferior de dispositivos de red, y el router que elige no tiene puertos serie (ver la explicación de cable serie un poco más abajo), tendrá que añadir una tarjeta de puertos serie en la pestaña Physical del router. Apague el router, añada una tarjeta WIC-2T, y encienda el router de nuevo. Si ha añadido el router copiando el Router1 esto no es necesario hacerlo.

Cable serie: El enlace que une los dos routers es un enlace serie. Este tipo de enlace se utiliza para simular la conexión de subredes en el nivel 3 a través de operadoras (líneas alquiladas). La particularidad de este tipo de enlace es que uno de los extremos debe proveer de una señal de sincronización. Indique en uno de los 2 lados del enlace serie que la sincronización será a 64000. Para determinar cuál es el extremo que debe aportar la sincronización, deje el cursor un instante sobre el enlace, el extremo que debe aportar la sincronización es el que está marcado con un símbolo de reloj.

Elimine la configuración de la dirección IP de la interfaz FastEthernet0/1 del Router1 (y del Router2 si la tiene) ya que ahora no estará conectada a ninguna subred.

Configure la dirección IP en las interfaces de los routers.

(Recuerde que la notación /24 equivale a la máscara de subred 255.255.255.0)

Cuando configure en los routers la interfaz Serial, asegúrese de que el puerto está activado (Port status = On), y si no es así, actívelo.

Tenga en cuenta que la configuración de PC1 y PC2 no ha variado, ya que siguen conectados a la misma subred que antes.

Rutas estáticas: Cuando un router tiene una interfaz directamente conectada a una subred, sabe que los paquetes que vayan a esa subred debe enviarlas por dicha interfaz. Sin embargo, ahora existen subredes mas allá del alcance de los routers: ahora **router1** no está conectado directamente a la subred a la que pertenece PC2, ni **router2** a la que pertenece PC1. Por lo tanto, debemos indicar en cada router cómo llegar a la subred a la que no está directamente conectado:

- Router1 ahora no está conectado directamente con la red del PC2. Debe entregar los paquetes a ella destinados a la interfaz serial de router2..
- Router2 ahora no está conectado directamente con la red del PC1. Debe entregar los paquetes a ella destinados a la interfaz serial de router1.

Por ahora esto lo vamos a hacer incorporando **rutas estáticas** en ambos routers. Una ruta es un camino para llegar a una subred. Una ruta estática es una ruta que se configura "a mano", y que no cambia.

Para ello acceda en cada router a **Config > Static** e introduzca la información siguiente pulsando luego al botón Añadir (Add):

En Router1: <subred de PC2> vía <IP interfaz serial router2>

En Router2: <subred de PC1> vía <IP interfaz serial router1>

Donde los campos de configuración significan lo siguiente:

- Network: Es la dirección IP de la subred (por ejemplo, 192.168.1.0).
- Mask: Es la máscara de red, que indica qué porción de la dirección de red identifica a los hosts. Recuerde que la máscara de subred es el "/24", que en formato de cuatro octetos es 255.255.255.0.
- Next Hop: Es hacia donde (o *vía* donde) hay que mandar los paquetes. Ahora mismo los dos routers están conectados por un cable y parece obvio que los tienen que mandar hacía el otro router, pero podría haber una conexión multi-punto y haber varios routers. Por ello, es necesario indicar la dirección IP de la interfaz del siguiente router (next hop) hacia donde se quiere que se envíen los paquetes. Observe bien que hay que indicar la

dirección IP del otro router, no la de la propia interfaz.

Realice estas configuraciones de encaminamiento en los dos routers de modo que se permita la comunicación entre subredes.

Para verificar la red, realice un ping entre PC1 y PC2. Realice varios pings si el primero falla, ya que el primer paquete que le llegue a cada router puede que éste lo descarte. En caso de que la red no funcione, compruebe los siguientes elementos por este orden:

1. **Existe conectividad física**: las interfaces están en verde y activas (situando el ratón sobre el equipo, Link = up) y conectadas a los puertos en los que han de estar conectados. Los enlaces serie tienen señal de sincronización.
2. **Existe conectividad en el nivel de red**: las interfaces de hosts y routers tienen la dirección IP y la máscara y todas son correctas; los hosts tienen bien configurado el router por defecto, también llamado gateway por defecto o sencillamente gateway (se ve poniendo el cursor encima del router, o picando en el router y 'Config > Settings'); las rutas estáticas están bien configuradas; los paquetes llegan hasta el router por defecto y lo atraviesan; los paquetes llegan de un router al siguiente, y atraviesan el siguiente.

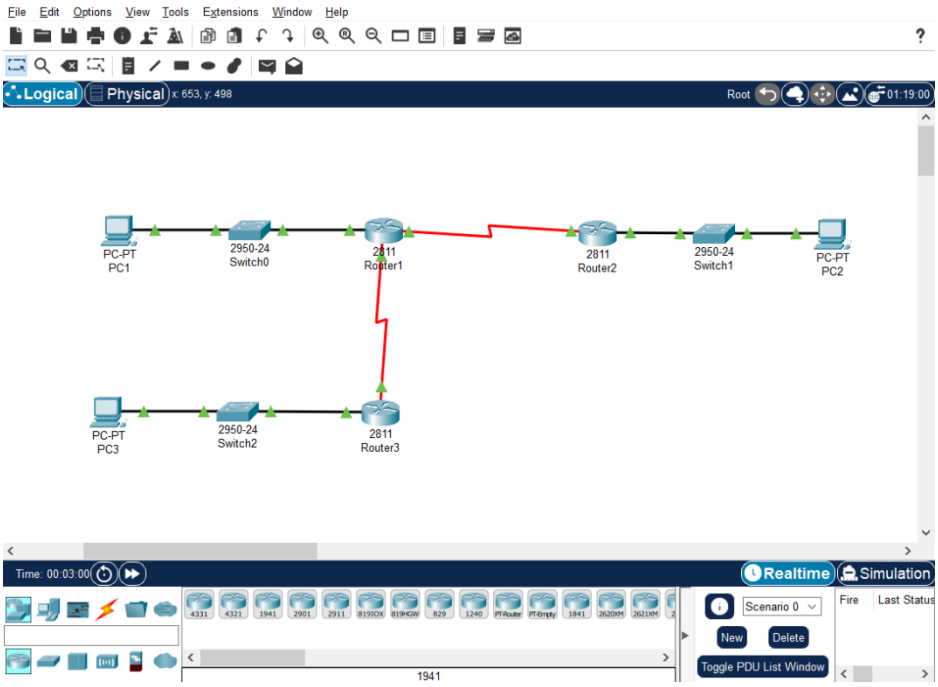
Una vez que consiga hacer funcionar la red, pase a la página siguiente.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas que requiere obtener y entender la tabla de encaminamiento de un router en packet tracer.

8.5 Caso 3: 5 subredes y 3 routers

Ahora vamos a incorporar a la configuración una subred que incluye un host y un router: PC3 y Router3. Esta subred se conectará con el Router1 a través de un enlace serie como el ya utilizado en la etapa anterior que conecte las interfaces Serial0/0/1 de ambos routers. Este enlace serie soportará otra subred de conexión.

Realice los pasos necesarios para crear y configurar una red similar a la de la figura siguiente.

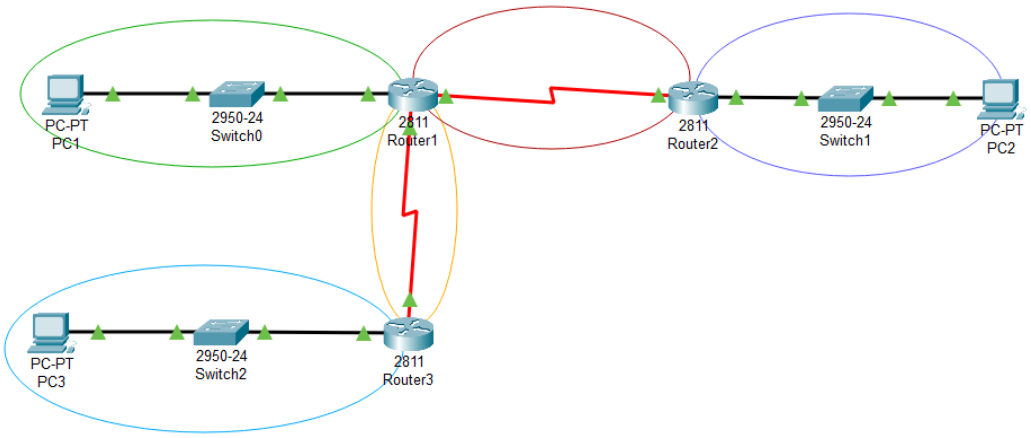


NOTA: Recuerde que puede seleccionar varios dispositivos y cables a la vez pinchando y arrastrando alrededor de ellos, para copiarlos y pegar después una copia. Pero no se olvide de cambiar la configuración de todos los dispositivos copiados (IPs de interfaces conectados, el gateway de los PCs en la sección de Settings, rutas estáticas en los routers, etc).

También, cuando configure en los routers la interfaz Serial, asegúrese de que el puerto está activado (Port status = On).

Para configurar el encaminamiento, deberá considerar para cada router las subredes que no son accesibles directamente. Por ejemplo, en el caso de Router3, deben indicarse las rutas para las 3 subredes que no están directamente conectadas. Para llegar a ellas el Router3 debe entregar los paquetes obligatoriamente a la interfaz del Router1 a la que está conectado. Del mismo modo, tendrá que añadir rutas estáticas a Router1 y Router2 para poder encaminar en la nueva configuración a las subredes que no están directamente conectadas.

Para mayor claridad, la siguiente imagen muestra con elipses las subredes existentes.



Pruebe que existe una conectividad total realizando pings entre los distintos hosts. Por ejemplo, PC3 - PC2, PC1 - PC3 y PC1 - PC2. Recuerde que puede que el primer paquete que le llega a un router éste lo descarte, por lo que haga varios pings para asegurar.

Es normal que a la primera no le funcione y haya algún error en la configuración. En caso de que la red no funcione, compruebe los siguientes elementos por este orden:

1. **Existe conectividad física**: las interfaces están en verde y activas (situando el ratón sobre el equipo, Link = up) y conectadas a los puertos en los que han de estar conectados. Los enlaces serie tienen señal de sincronización.
2. **Existe conectividad en el nivel de red**: las interfaces de hosts y routers tienen la dirección IP y la máscara y todas son correctas; los hosts tienen bien configurado el router por defecto, también llamado gateway por defecto o sencillamente gateway (se ve poniendo el cursor encima del router, o picando en el router y 'Config > Settings'); las rutas estáticas están bien configuradas; los paquetes llegan hasta el router por defecto y lo atraviesan; los paquetes llegan de un router al siguiente, y atraviesan el siguiente.

Sobre todo, revise la configuración en los nuevos elementos: Dirección IP y default gateway en PC3; dirección IP en las dos interfaces de Router3; dirección IP en la nueva interfaz serial de Router1. Es bueno que si no le funciona, active el modo simulación, seleccione el filtro ICMP, y vea dónde se pierden los paquetes, eso le dará pistas de dónde hay algún error de configuración.

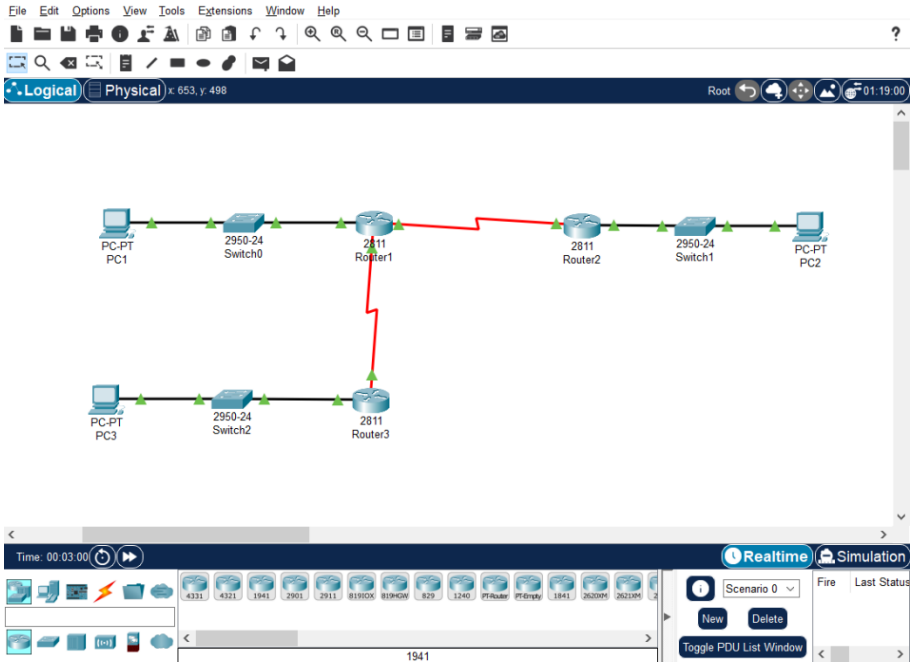
Una vez que la red esté configurada y funcionando, responda a las siguientes preguntas.

> Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas sobre las tablas de rutas de los routers del escenario anterior.

8.6 Caso 4: 5 subredes y 3 routers (con ruta por defecto)

En este paso trataremos de simplificar las tablas de enrutamiento de los routers mediante la inclusión de la ruta por defecto en ellas.

Fíjese en el caso del Router3 de la red en la siguiente figura.



Desde Router3, las rutas que deben seguir cualquier paquete destinado a las subredes del PC1, del PC3 y de la conexión serial entre Router1 y Router2 pasan obligatoriamente por el Router1, lo que se expresa explícitamente con rutas estáticas. Observe cuántas rutas estáticas necesita, tanto en 'Config > Static', como ejecutando el comando 'show ip route' en modo CLI.

Este listado de rutas estáticas se puede simplificar indicando una **ruta por defecto** para las subredes no directamente conectadas. En este caso, Router3 puede resumir esas rutas con una ruta por defecto que pasa por la interfaz del Router1 a la que está conectado.

Una ruta por defecto es una ruta que se define **para cualquier destino**. Hay que tener en cuenta que si un router tiene una ruta estática "más específica", por ejemplo, para el destino 192.168.1.0/24, y una ruta por defecto, aunque ambas rutas aplicarían para dicho destino, siempre tiene prioridad la más específica. La ruta por defecto se usará si no se encuentra otra ruta para ese destino.

Algo similar sucede para Router2 con respecto a las rutas con destino a las subredes del PC1, del PC2 y de la conexión serial entre Router1 y Router3, que pueden ser resumidas indicando una ruta por defecto hacia la IP de la interfaz de Router1 a la que está conectado Router2.

En el caso del Router1, resulta que él es el router central de toda la red, de modo que resulta el router por defecto tanto para Router2 como para Router3. En cierto modo, él tiene un conocimiento más completo de las rutas a todas las subredes de toda la red. Reflexione si Router1 debe tener alguna ruta por defecto en este caso.

La configuración de una ruta por defecto se indica colocando 0.0.0.0 tanto en el campo "Network" (0.0.0.0 significa *cualquier IP*) como en el "Mask" (0.0.0.0 significa *cualquier máscara*), indicando la dirección IP de la interfaz del siguiente router en el campo de "Next Hop".

Modifique la información de encaminamiento de los routers para **incluir las rutas por defecto y poder borrar las que ya no hacen falta**.

Verifique el funcionamiento de la red repitiendo el ping entre todos los hosts. En caso de que la red no funcione, compruebe los siguientes elementos por este orden:

1. **Existe conectividad física**: las interfaces están activas y conectados a los puertos en los que han de estar conectados. Los enlaces serie tienen señal de sincronización.
2. **Existe conectividad en el nivel de red**: las interfaces de hosts y routers tienen la dirección IP y la máscara y todas son correctas; los hosts tienen bien configurado el router por defecto, también llamado gateway por defecto o sencillamente gateway (se ve poniendo el cursor encima del router, o picando en el router y 'Config > Settings'); las rutas estáticas están bien configuradas; los paquetes llegan hasta el router por defecto y lo atraviesan; los paquetes llegan de un router al siguiente, y atraviesan el siguiente.

Sobre todo, revise la configuración de las rutas estáticas, ya que es lo nuevo que ha cambiado. Es bueno que si no le funciona, active el modo simulación, seleccione el filtro ICMP, y vea dónde se pierden los paquetes, eso le dará pistas de dónde hay algún error de configuración.

Una vez que todo esté correctamente configurado, responda a la siguiente pregunta.

> Aquí se incluye pregunta aleatoria de un banco de preguntas sobre la ruta por defecto en un router del escenario anterior.

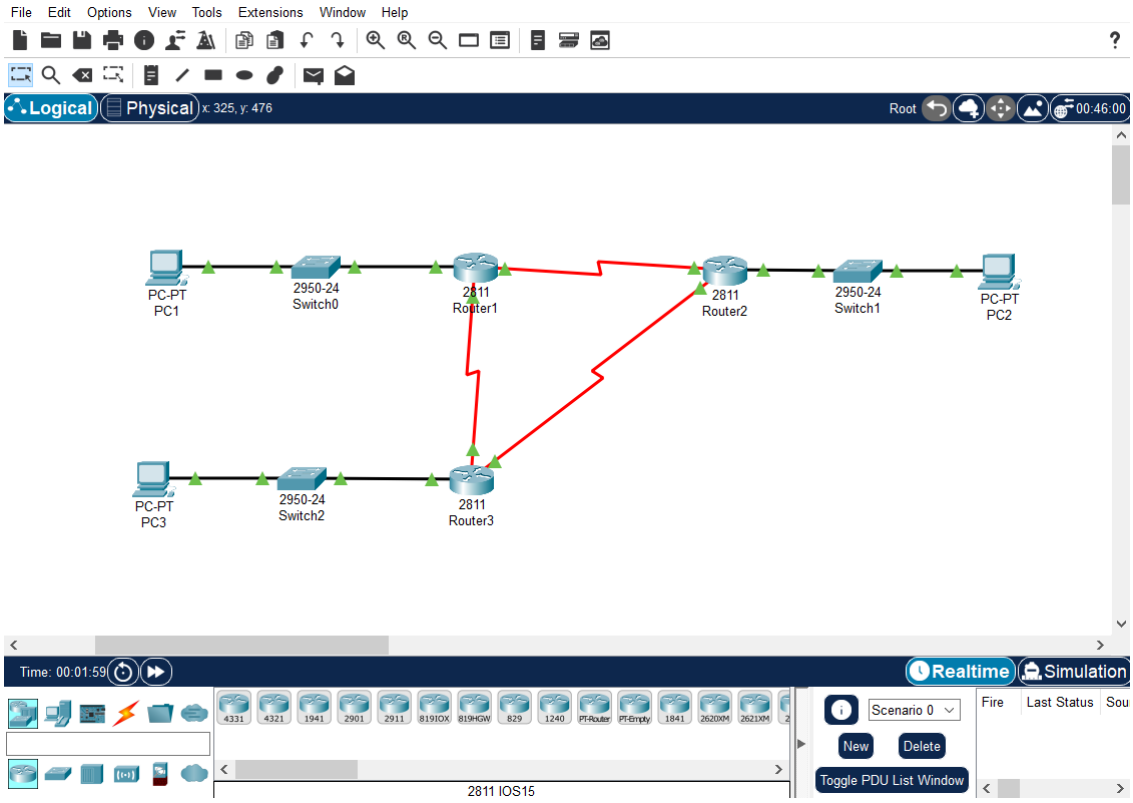
8.7 Caso 5: 6 subredes, 3 routers y RIP

Ahora vamos a incluir el encaminamiento dinámico en nuestra red.

En el caso anterior, ya hemos visto que se incrementa rápidamente la complejidad de la correcta configuración de las rutas estáticas cuando la red crece un poco en complejidad. Además, no hemos considerado el problema que supondrá modificar las rutas por la caída de un enlace o de un router.

Es el momento de introducir el encaminamiento dinámico utilizando el protocolo RIP en nuestra pequeña red de laboratorio, a la vez que completamos la conexión entre los 3 routers con un nuevo enlace serie entre router2 y router3. Habrá una nueva subred añadida entre los routers 2 y 3, que introduce un camino redundante en la red.

Realice las acciones necesarias para que la red resultante resulte similar a la representada en la siguiente figura.



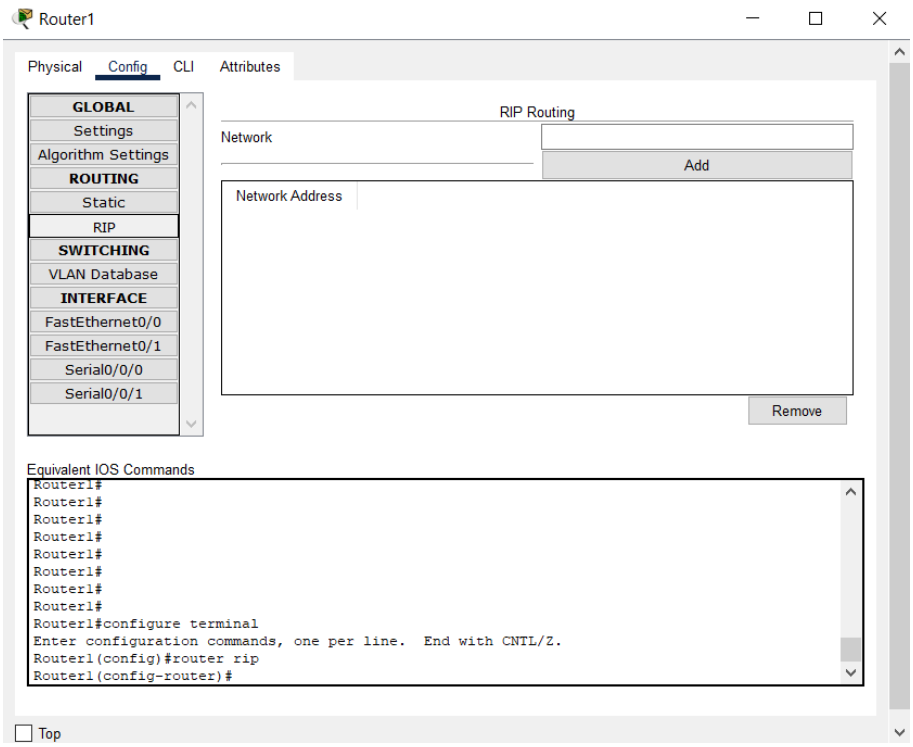
Cuando configure en los routers la interfaz Serial, atienda a configurar correctamente la sincronización en el enlace, y asegúrese de que el puerto está activado (Port status = On).

Tenga en cuenta que con la nueva red, aunque ahora tiene un camino redundante que podría servir en el caso de que cayera alguno de los enlaces serial anteriores, como las rutas estáticas en Router2 y Router3 apuntan a Router1, el nuevo enlace no se usaría. Para que se usase, deberían configurarse rutas estáticas para los caminos alternativos. Esto complica mucho la configuración. Un protocolo dinámico de routing hace que los routers se envíen la información de rutas de forma que en cada router la tabla de encaminamiento se rellena dinámicamente, además de con la información local (directamente conectadas o estáticas), con la "aprendida" de otros routers.

En nuestro caso, para la configuración de las tablas de encaminamiento de los routers vamos a configurar ahora el protocolo de encaminamiento dinámico RIP.

En cada router, elimine las rutas estáticas e introduzca en la configuración de RIP **las redes directamente conectadas**. Las redes que configure en RIP serán anunciadas por el router a los demás routers usando el protocolo de encaminamiento dinámico RIP. El router sólo anunciará redes que estén configuradas en RIP y que estén directamente conectadas, o redes que haya aprendido de otros routers.

En la figura siguiente se muestra dónde debe añadir la información de encaminamiento para el caso de Router1. El protocolo RIP se encargará de intercambiar dicha información entre los routers vecinos hasta alcanzar toda la red.



Una vez configurado, los routers se intercambiarán periódicamente la información de encaminamiento (la tabla de rutas). El tiempo que tarda la red en que todos los routers tengan la información de rutas actualizada se denomina tiempo de convergencia. RIP tarda del orden de bastantes segundos en converger, es relativamente lento.

Compruebe el correcto funcionamiento de la red, realizando pings entre las distintas zonas de la misma. En caso de que la red no funcione, compruebe los siguientes elementos por este orden:

1. **Existe conectividad física**: las interfaces están activas (situando el ratón sobre el equipo, Link status = up) y conectadas a los puertos en los que han de estar conectados. Los enlaces serie tienen señal de sincronización.
2. **Existe conectividad en el nivel de red**: las interfaces de hosts y routers tienen la dirección IP y la máscara y todas son correctas; los hosts tienen bien configurado el router por defecto, también llamado gateway por defecto o sencillamente gateway (se ve poniendo el cursor encima del router, o picando en el router y 'Config > Settings'); las rutas estáticas están eliminadas; están configuradas en RIP las rutas directamente conectadas; los paquetes llegan hasta el router por defecto y lo atraviesan; los paquetes llegan de un router al siguiente, y atraviesan el siguiente.

Sobre todo, revise la configuración de rutas estáticas y RIP, ya que es lo nuevo que ha cambiado. Es bueno que si no le funciona, active el modo simulación, seleccione el filtro

ICMP, y vea dónde se pierden los paquetes, eso le dará pistas de dónde hay algún error de configuración.

Una vez que la red funcione correctamente, responda a las siguientes preguntas.

> Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requiere entender el encaminamiento obtenido por RIP que aparece en la tabla de rutas, así como observar en la red la diferencia entre encaminamiento estático y dinámico por RIP.

8.8 Investigando...

Enhorabuena por haber conseguido llegar al final Si dispone de un poco de tiempo extra, aproveche la ocasión para investigar por su cuenta. Realice cambios en la configuración y observe si la red sigue funcionando correctamente.

Sugerencia:

Analice el contenido de los mensajes RIP intercambiados.

Investigue sobre el tiempo necesario para que RIP converja en esta red.

Guarde el archivo con la red en este estado para su posterior estudio.

9. VLANs y encaminamiento

9.1 Introducción y Objetivos

En este ejercicio, se trata de iniciarse en el diseño y configuración de VLANs configurando dos de sus elementos fundamentales: **switches** y **routers**.

En este caso, la definición de VLAN vendrá dada de forma estática por medio de los puertos de entrada del switch. En un principio, el router, el otro elemento importante en este caso, tendrá una interfaz de red conectada a cada una de las VLANs, y realizará las funciones de encaminamiento entre las distintas VLANs. Hay que recordar que normalmente cada VLAN estará asociada a una subred distinta, lo que implicará que el router deberá tener una interfaz de red conectada a cada una de las subredes que deba encaminar.

En este modo de conexión básico, el modelo de VLAN no resultará demasiado escalable, ya que el número de VLANs (y por lo tanto de subredes) a considerar estará limitado por el número de interfaces de red que tenga el router.

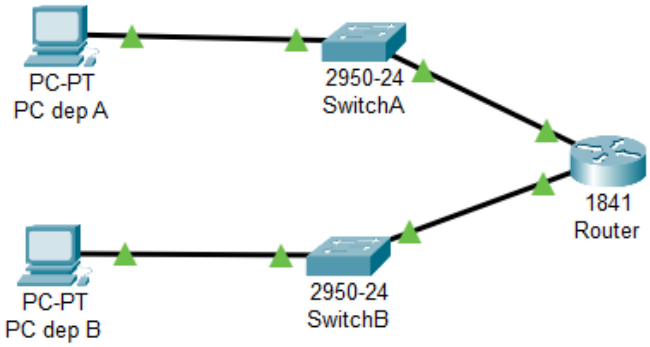
Para resolver esto se introducen dos elementos fundamentales: el modo *trunk* en los enlaces, y las subinterfaces en el router. Esto permitirá que un único enlace pueda transportar tráfico asociado a varias VLANs, y que una única interfaz de red física pueda recibir tráfico de varias subredes distintas, a través de varias subinterfaces (o interfaces virtuales asociadas a una interfaz física).

El ejercicio de laboratorio que ahora comienza va a ilustrar esto de modo incremental, proponiendo la realización de distintos escenarios en los que se irán incorporando estos elementos de manera sucesiva.

9.2 CASO 1: 2 subredes, 2 switches y dos interfaces de red en el router

En este escenario de partida se construirá una red básica con dos subredes, cada una soportada por un switch distinto y conectadas por un router con una interfaz de red conectada a cada subred.

Reproduzca el caso representado en la figura y configure las direcciones IP de las interfaces de los PCs y el router:



Recuerde que tiene que poner a ON los puertos del router.

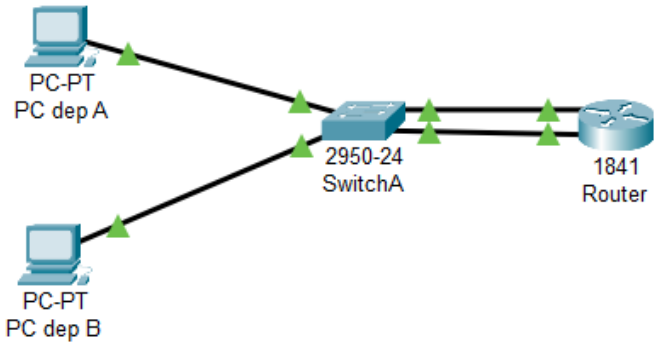
Compruebe que todo funciona realizando pings entre PC dep A y PC dep B. Fíjese el camino que toman los paquetes en dichos pings (modo simulación).

Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre las VLANes asociadas en los puertos de los switches

9.3 CASO 2: un switch

En este segundo caso, vamos a sustituir los dos switches por uno sólo soportando dos VLANs, cada una asociada a la subred que anteriormente soportaban los dos switches.

Reproduzca la red de la figura sin configurar todavía VLANes:



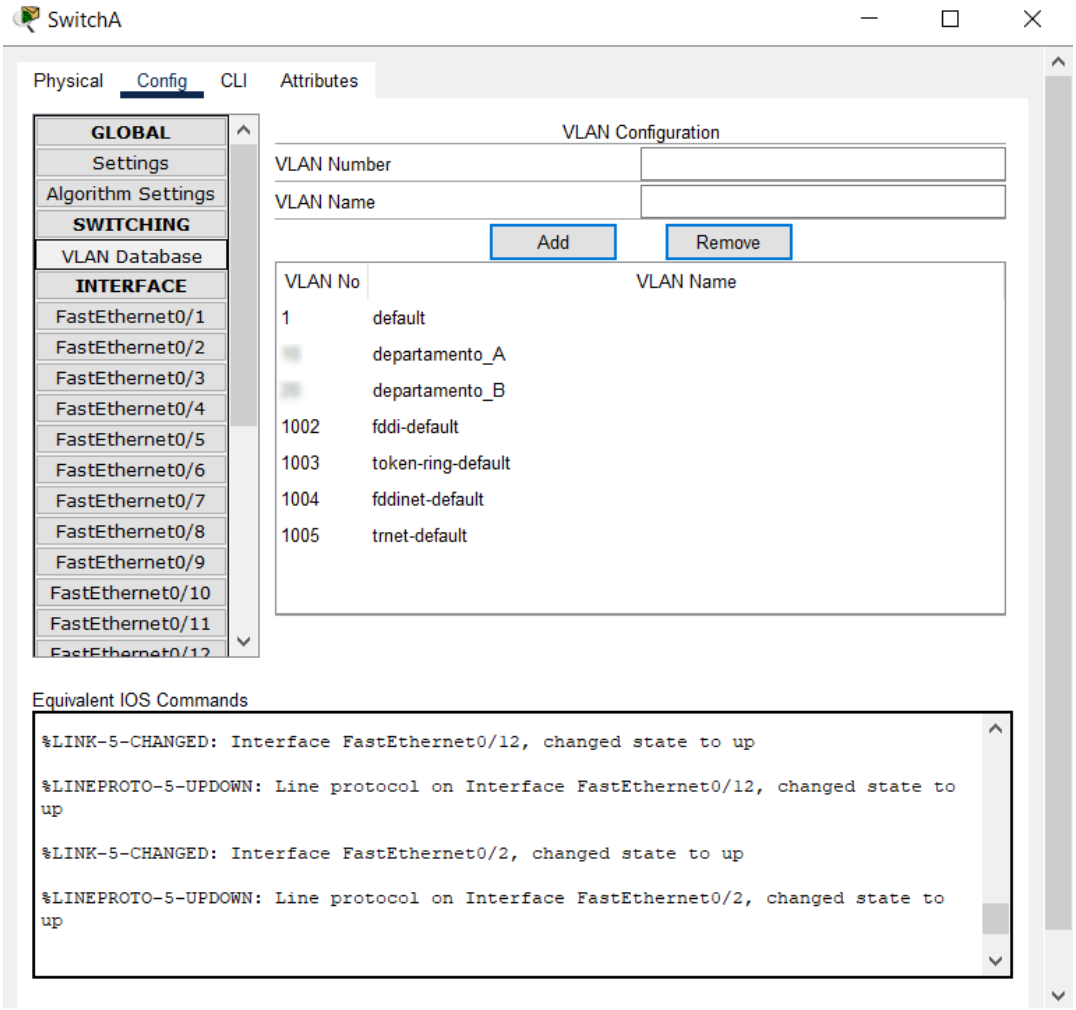
Aún no hemos introducido VLANs en el switch, por lo que los dos hosts y el router están en el mismo dominio de difusión. Compruebe esto en el modo simulación provocando la emisión de paquetes IP de difusión (broadcast), por ejemplo, colocando uno de los hosts en modo DHCP (no se preocupe si todos los paquetes DHCP fallan, ya que no hay servidor DHCP). Recuerde volver a la configuración IP estática una vez estudiando el dominio de difusión. Esos paquetes llegan a todos los nodos conectados, independientemente de la subred a la que pertenezcan, pues el switch reenvía los paquetes de difusión por todos los puertos activos que tenga. Esto se puede convertir en una tormenta de difusión que afectaría a todos los nodos y segmentos de red conectados al switch si varios nodos encadenan envíos de broadcast.

9.4 Creación de VLANs y configuración de los puertos del switch

Ahora vamos a proceder a crear las VLANs y a configurar los puertos del switch adecuadamente.

En la pestaña de configuración del switch, seleccione la base de datos de VLAN. Añada dos VLANs, una para la subred del departamento A, y otra para la subred del departamento B. Aunque el número de las VLANs no tiene relación con la dirección IP de las subredes que soportarán, es una buena idea mantener un esquema de numeración coherente entre estos dos elementos.

El resultado final debería parecerse al de la siguiente figura.



Ahora hay que proceder a asociar los puertos del switch conectados a los PCs y al router a una de las VLANs creadas. En las ventanas de configuración de dichos puertos asigne las correspondientes VLANs.

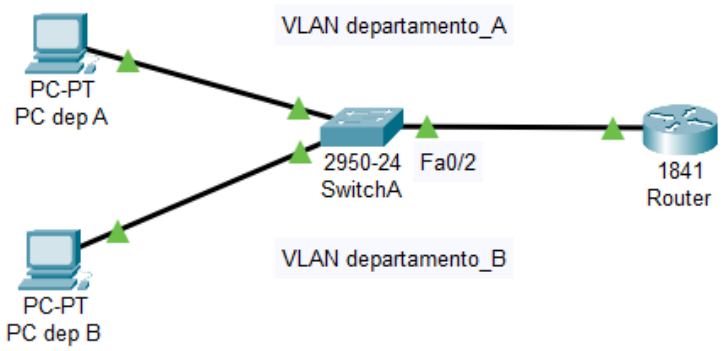
Compruebe que todo funciona correctamente y que ahora existen varios dominios de difusión. Para ello, en modo simulación, observe el camino de los paquetes de difusión que emiten los distintos nodos de la red.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre los dominios de difusión de la red anterior

9.5 CASO 3: subinterfaces

En este tercer caso, el router va a conectarse al switch utilizando únicamente una interfaz de red: en este caso la interfaz **FastEthernet0/0**. Esta única interfaz de red debe ser capaz de atender a las dos subredes teniendo una dirección IP de cada una, y esto va a ser posible mediante la creación de dos subinterfaces (interfaces virtuales) en el puerto físico, y la asignación a cada una de ellas la dirección IP en la subred correspondiente.

Reproduzca el diseño que aparece en la figura a partir del diseño del CASO 2. Para ello desactive las interfaces del router conectadas al switch, eliminando también la configuración de las mismas. Elimine también el enlace ethernet de abajo que conecta con el switch, para dejar sólo uno. **No debe modificar la configuración existente en el switch, al menos de momento,** pues esto podría afectar a las respuestas.



Para conseguir la configuración del router (con las dos interfaces de red desactivadas y sin configuración) tenemos que acceder a la interfaz de comandos (CLI) del router e introducir la siguiente secuencia de comandos partiendo del estado inicial:

(Debe llevar al router al estado inicial, introduciendo tantos comandos exit como sea necesario hasta que se muestre el prompt Router>.El mismo comando **exit** servirá para dejar la configuración de una interfaz y pasar a la siguiente.)

Comando	Comentario
Router>**enable**	Pasar a modo supervisor. Observe el cambio en el prompt: Router#

Router#**configure terminal**	Configuración desde el terminal. Observe el cambio en el prompt: Router(config)#
Router(config)#**interface fastethernet <slot/puerto>**	Acceder a la configuración de la interfaz fastethernet <slot/puerto>.
Router(config-if)#**no shutdown**	Levantar la interfaz (se suponía desactivada)
Router(config-if)#**interface fastethernet <slot/puerto.subint>**	Acceder a la configuración de la subinterfaz fastethernet <slot/puerto.subint> para el departamento_A
Router(config-subif)#**encapsulation dot1q <VLAN_ID>**	Indicar que dicha subinterfaz <slot/puerto.subint> estará asociada a la vlan con ID del departamento_A. Los paquetes que salgan de ella estarán coloreados con la etiqueta correspondiente
Router(config-subif)#**ip address <IP> <mascara>**	Asignar a la subinterfaz la dirección IP y la máscara adecuadas en la subred del departamento_A. Teclee **exit** para salir de la configuración de esta interfaz y pasar a la siguiente.
Router(config-subif)#**interface fastethernet <slot/puerto.subint>**	Acceder a la configuración de la subinterfaz fastethernet <slot/puerto.subint> para el departamento_B
Router(config-subif)#**encapsulation dot1q <VLAN_ID>**	Indicar que dicha subinterfaz <slot/puerto.subint> estará asociada a la vlan con ID del departamento_B. Los paquetes que salgan de ella estarán coloreados con la etiqueta correspondiente
Router(config-subif)#**ip address <IP> <mascara>**	Asignar a la subinterfaz la dirección IP y la máscara adecuadas en la subred del departamento_B.
Router(config-subif)#**end**	finalizar la configuración

Para comprobar la configuración puede mantener el cursor sobre el router, y dicha configuración se mostrará en una ventana. También puede ejecutar el comando show running-config desde la interfaz de comandos (desde el modo supervisor, recuerde que el prompt debe indicar Router#). Dicha información debe mostrar las dos subinterfaces con la

información IP correcta. Si no fuera así, vuelva a realizar los pasos adecuados para que así sea.

Para que esta configuración en ejecución permanezca en el tiempo y sea la que se considere en el siguiente momento en que se arranque el router debe ser copiada a la configuración de arranque. Para ello ejecute el siguiente comando desde el modo supervisor:

Router# copy running-config startup-config

(Esto es equivalente a guardar la configuración del router en modo gráfico, como hemos hecho en prácticas anteriores)

Una vez que la configuración es correcta, pase a la siguiente página.

> Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas sobre la red anterior.

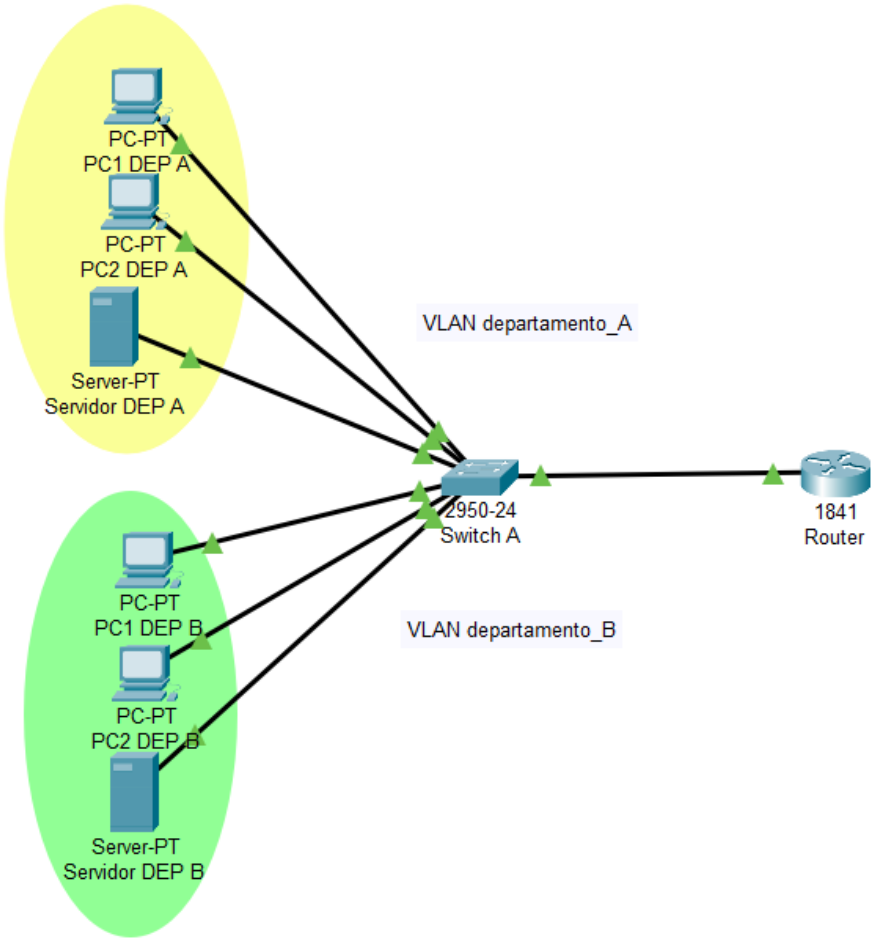
Para que la red funcione el switch debe ser capaz de hacer llegar los paquetes desde la subred del departamento_A a la del departamento_B y viceversa, y eso es imposible pues no existe ninguna VLAN que tenga conectados nodos de esas dos subredes. En el caso concreto de un ping de PCdepB a PCdepA, el resultado es que el paquete no puede salir del nodo PCdepB porque ni siquiera es capaz de alcanzar su router por defecto, ya que la interfaz del switch conectada al router está configurada en modo acceso y sólo transporta paquetes de la VLAN del departamento_A.

Para que la red funcione correctamente falta colocar el puerto del swith que conecta con el router en modo **trunk**. De ese modo ese puerto será capaz de gestionar el tráfico en cualquier VLAN. Vaya a la etiqueta de la interfaz correspondiente del switch (donde está conectado el router) y coloque el puerto en modo trunk. Ahora este puerto conducirá el tráfico de todas las VLANs existentes.

Compruebe que la red funciona, y el router encamina.

> Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre los dominios de difusión de la red anterior.

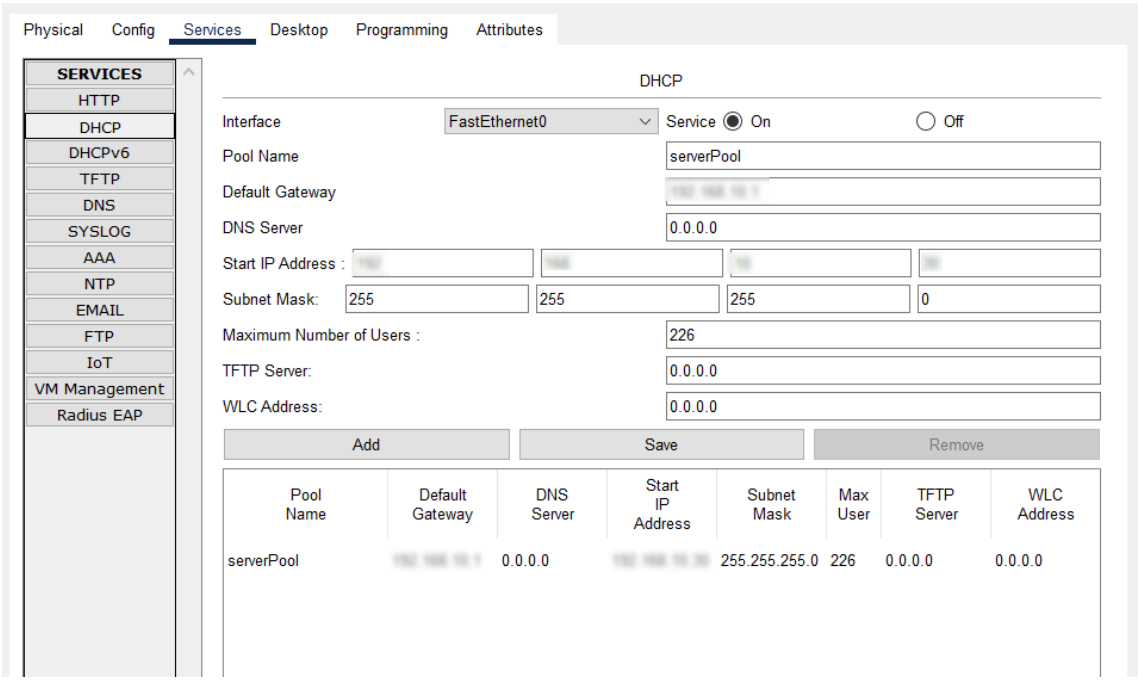
Construya la siguiente red, **reutilizando la anterior**:



En dicha red existen 2 vlans. Cada una de las vlans soporta una subred, en la que existe un servidor DHCP y uno o varios clientes DHCP. En este caso, los hosts de las subredes están dispersos geográficamente y conectados al mismo switch, pero las VLANs permiten que se mantengan separados los dominios de difusión de cada una de las subredes existentes.

Realice las configuraciones necesarias para conseguir que la red funcione correctamente. Apóyese en las configuraciones del caso anterior. Ponga especial atención al tipo de los enlaces (access/trunk) en el switch y las vlans que transporta cada enlace, para hacer que las solicitudes y respuestas de DHCP alcancen servidores y clientes, respectivamente.

Configure cada servidor de DHCP como muestra la siguiente figura (tendrá que configurar en cada departamento la subred correspondiente). Fíjese bien en lo que está configurando, es importante que entienda lo que está haciendo:



Y asegúrese que los clientes (los PCs) están configurados para DHCP y reciben una configuración correcta.

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas sobre VLANes, Ethernet y 802.1q.

Aquí se incluye una pregunta final de autorreflexión y síntesis sobre la práctica realizada y los conocimientos adquiridos.

10. Filtrado de paquetes en cortafuegos

En este ejercicio de laboratorio se muestra el modo en que podemos implementar cortafuegos que limitan el tráfico que puede acceder o salir de las redes dependiendo del tipo de tráfico. Esta funcionalidad proviene de las capacidades de los routers actuales, que pueden filtrar las peticiones de enrutado en función del tipo de tráfico. Junto a las pasarelas de aplicación, constituyen la plataforma básica de creación de cortafuegos (*firewall*) en la red.

Los routers de CISCO no son una excepción a ello, y aprovecharemos sus mecanismos basados en listas de control de acceso (ACL, *access control lists*) para implementar distintas configuraciones, entre las que destaca la creación de una zona desmilitarizada sencilla (DMZ, demilitarized zone). Como veremos, los routers CISCO permiten dos tipos de ACL: estándar (que permiten filtrar por origen) y extendidas (que permiten filtrar por origen y destino).

Los bloques que contempla esta lección son:

- Breve introducción a las listas de control de acceso.
- Descripción de un caso de creación de una red asegurada donde se aborda:
    - la descripción de los requisitos de seguridad de la red de una entidad;
    - cómo proteger la red corporativa mediante firewall;
    - cómo proteger la DMZ; y
    - cómo disuadir el spoofing.

Si necesitas más información sobre ACLs de Cisco puedes consultar los siguientes recursos:

- CCNA Free Study Guide. Chapter 9 – Access Lists
- MONOGRÁFICO: Listas de control de acceso (ACL) - Utilización de ACLs en routers
- Cisco: Configurar ACL de IP de uso general

10.1 Breve presentación de las ACLs[1]

Las ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router. Estas listas le informan al router qué tipo de paquetes aceptar o rechazar. La aceptación y rechazo se pueden basar en ciertas condiciones específicas.

Las ACL permiten la administración del tráfico y aseguran el acceso hacia y desde una red. Las ACL filtran el tráfico de red, controlando si los paquetes enrutados se envían o se

[1] Extraído del Cisco Networking Academy Program CCNA 2

bloquean en las interfaces del router. El router examina cada paquete y lo enviará o lo descartará, según las condiciones especificadas en la ACL. Algunos de los puntos de decisión de ACL son direcciones origen y destino, protocolos y números de puerto de capa superior.

Estas son las razones principales para crear las ACL:

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de video, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Brindar control de flujo de tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le niega el acceso a dicha red.
- Previa decisión de los tipos de tráfico que se envían o bloquean en las interfaces del router, permitir que se enrute el tráfico de correo electrónico, pero bloquear todo el tráfico de telnet.
- Permitir que un administrador controle a cuáles áreas de la red puede acceder un cliente.
- Analizar ciertos hosts para permitir o denegar acceso a partes de una red.
- Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

Si las ACL no están configuradas en el router, todos los paquetes que pasen a través del router tendrán acceso a todas las partes de la red.

El orden en el que se ubican las sentencias (o *statements*) de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo. Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo.

Si se requieren más cantidad de sentencias de condición en una lista de acceso, se debe borrar y volver a crear toda la ACL con las nuevas sentencias de condición.

A manera de revisión, las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si todas las sentencias ACL no tienen coincidencias, se coloca una sentencia implícita que dice **deny any** (denegar cualquiera) en el extremo de la lista por defecto. Aunque la línea **deny any** no sea visible como última línea de una ACL, está ahí y no permitirá

que ningún paquete que no coincida con las líneas anteriores de la ACL sea aceptada. Cuando esté aprendiendo por primera vez cómo crear una ACL, es una buena práctica agregar el **deny any** al final de las ACL para reforzar la presencia dinámica de la prohibición implícita **deny**.

En TCP/IP, las ACL se asignan a una o más interfaces y pueden filtrar el tráfico entrante o saliente.

Es necesario utilizar estas reglas básicas a la hora de crear y aplicar las listas de acceso.

1. Se deben aplicar las listas de acceso estándar que se encuentran lo más cerca posible del destino.
2. Se deben aplicar las listas de acceso extendidas que se encuentran lo más cerca posible del origen.
3. Utilice la referencia de la interfaz entrante y saliente como si estuviera mirando el puerto desde adentro del router.
4. Las sentencias se procesan de forma secuencial desde el principio de la lista hasta el final hasta que se encuentre una concordancia, si no se encuentra ninguna, se rechaza el paquete.
5. Hay un **deny any** (denegar cualquiera) implícito al final de todas las listas de acceso. Esto no aparece en la lista de configuración.
6. Las entradas de la lista de acceso deben realizar un filtro desde lo particular a lo general. Primero se deben denegar hosts específicos y por último los grupos o filtros generales.
7. Primero se examina la condición de concordancia. El permiso o rechazo se examina SÓLO si la concordancia es cierta.
8. Nunca trabaje con una lista de acceso que se utiliza de forma activa.
9. Utilice el editor de texto para crear comentarios que describan la lógica, luego complete las sentencias que realizan esa lógica.
10. Siempre, las líneas nuevas se agregan al final de la lista de acceso. El comando **no access-list** elimina toda la lista. No es posible agregar y quitar líneas de manera selectiva en las ACL numeradas.
11. Una lista de acceso IP envía un mensaje ICMP llamado de host fuera de alcance al emisor del paquete rechazado y descarta el paquete en la papelera de bits.
12. Se debe tener cuidado cuando se descarta una lista de acceso. Si la lista de acceso se aplica a una interfaz de producción y se la elimina, según sea la versión de IOS, puede haber una **deny any** (denegar cualquiera) por defecto aplicada a la interfaz, y se detiene todo el tráfico.
13. Los filtros salientes no afectan al tráfico que se origina en el router local.

10.1.1 Sintaxis

La sintaxis completa del comando *ACL estándar* es:

```
Router(config)# access-list access-list-number {deny | permit | remark} source [source-wildcard] [log]
```

Las *ACL extendidas* se utilizan con más frecuencia que las ACL estándar porque ofrecen un mayor control. Las ACL extendidas verifican las direcciones de paquetes de origen y destino, y también los protocolos, números de puerto, etc.

```
Router(config)# access-list access-list-number {deny | permit | remark} { protocolo tpc/udp/icmp/... } source [source-wildcard] [destination [destination-wildcard]] [ { established | eq puerto | tipo_mensaje } ] [log]
```

10.1.2 Máscara de wildcard

Las máscaras de *wildcard* se usan en lugar de las direcciones de source o destination. Usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros. Un **0** significa que se deje pasar el valor para verificarlo. Los **1** significan impedir que se compare el valor (lo que en la práctica equivale a utilizar un comodín "**?**").

Hay dos palabras clave especiales que se utilizan en las ACL, las opciones **any** y **host**, que se utilizan en lugar de dirección y máscara de origen y/o destino. Para explicarlo de forma sencilla, la opción **any** reemplaza la dirección IP con 0.0.0.0 y la máscara *wildcard* por 255.255.255.255. Esta opción admite cualquier dirección con la que se la compare. En la opción **host** la máscara es 0.0.0.0. Esta máscara necesita que se indiquen todos los bits de la dirección de la máquina y por tanto admite paquetes sólo de esa dirección IP.

10.1.3 Aplicación de ACLs

El comando **ip access-group** enlaza una ACL extendida existente a una interfaz. Recuerde que sólo se permiten dos ACL por interfaz y protocolo, una para los paquetes de entrada, y otra para los de salida. El formato del comando es:

```
Router(config-if)#ip access-group access-list-number {in | out}
```

***Atención**: Una ACL que contiene sentencias ACL numeradas no puede ser alterada. Se debe borrar utilizando el comando* **no access-list** *list-number* y entonces proceder a recrearla.

10.1.4 Mostrar la información sobre las ACL

El comando **show ip interface** muestra información de la interfaz IP e indica si se ha establecido alguna ACL. El comando **show access-lists** muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número ACL como opción a este comando. El comando **show running-config** también revela las listas de acceso en el router y la información de asignación de interfaz.

10.2 Supuesto práctico

El ejercicio de laboratorio va a estudiar el caso de una empresa que quiere dar a conocer sus productos a través de Internet. El requisito inmediato es promocionar sus productos entre los clientes potenciales proporcionando datos generales sobre los mismos a través de un portal web. Los requisitos futuros podrían incluir servicios de correo electrónico, FTP, DNS y comercio electrónico.

La empresa te ha contratado para diseñar y configurar una infraestructura de seguridad para dar soporte a sus requisitos de red internos y externos sin perder de vista los costes.

Un análisis cuidadoso te convence de la necesidad de crear una arquitectura en dos zonas consistente en una zona de red corporativa y una DMZ (zona desmilitarizada). La primera albergará los servidores privados y los clientes internos. La DMZ alojará sólo un servidor web.

En este escenario, sigue metódicamente cada uno de los casos que se te plantean a continuación.

10.3 Configuraciones básicas

Realiza las configuraciones básicas necesarias para conseguir una red como la mostrada en la figura siguiente. No se olvide de añadir el módulo de interfaces serie en el slot adecuado del router (en la pestaña Physical de la configuración) para que la notación de dicha interfaz sea "Serial 0/0/0" y poder utilizar cable serie entre los routers (para más detalle de cómo se realiza esto, ver la Figura 2, un poco más abajo).

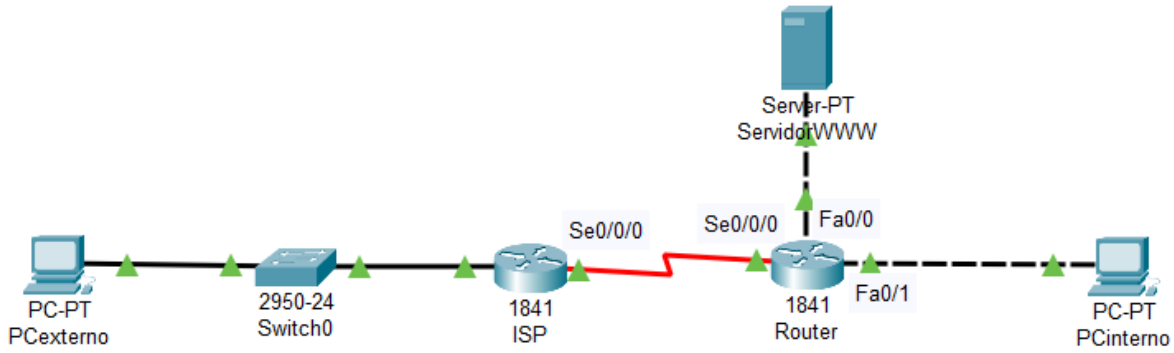


Figura 1. Topología de red para la práctica

Los datos de configuración son los siguientes:

- **Routers**:

	Dirección IP FastEthernet0/0	**Dirección IP FastEthernet0/1**	**Dirección IP Serial0/0/0**
Router	192.168.1.1/24	192.168.10.1/24	192.168.161.2/24
ISP	192.168.162.1/24	n/a	192.168.161.1/24

- **Encaminamiento RIP** (Config > RIP):

	Protocolo	**Networks**
Router	**RIP**	192.168.1.0, 192.168.10.0 y 192.168.161.0
ISP	**RIP**	192.168.161.0 y 192.168.162.0

- **Hosts**:

Host	**Dirección IP**	**Máscara de subred**	**Default Gateway**
Servidor WWW	192.168.1.10	255.255.255.0	192.168.1.1
PC Interno	192.168.10.10	255.255.255.0	192.168.10.1
PC Externo	192.168.162.10	255.255.255.0	192.168.162.1

Para añadir el módulo de interfaces serie al router, hay que entrar en la pestaña "Physical" del router, y hacer lo siguiente (ver Figura 2):

1. Apagar el router (no se pueden insertar o extraer tarjetas con el router encendido porque se pueden dañar tanto la tarjeta como el router).
2. Arrastrar el módulo de interfaces serie al slot correspondiente (tener en cuenta que la interfaz tiene que ser Se0/0/0, y en un router cisco 1841 el formato de la numeración es: serial 0/<nº slot>/<nº interfaz>).
3. Encender de nuevo el router.

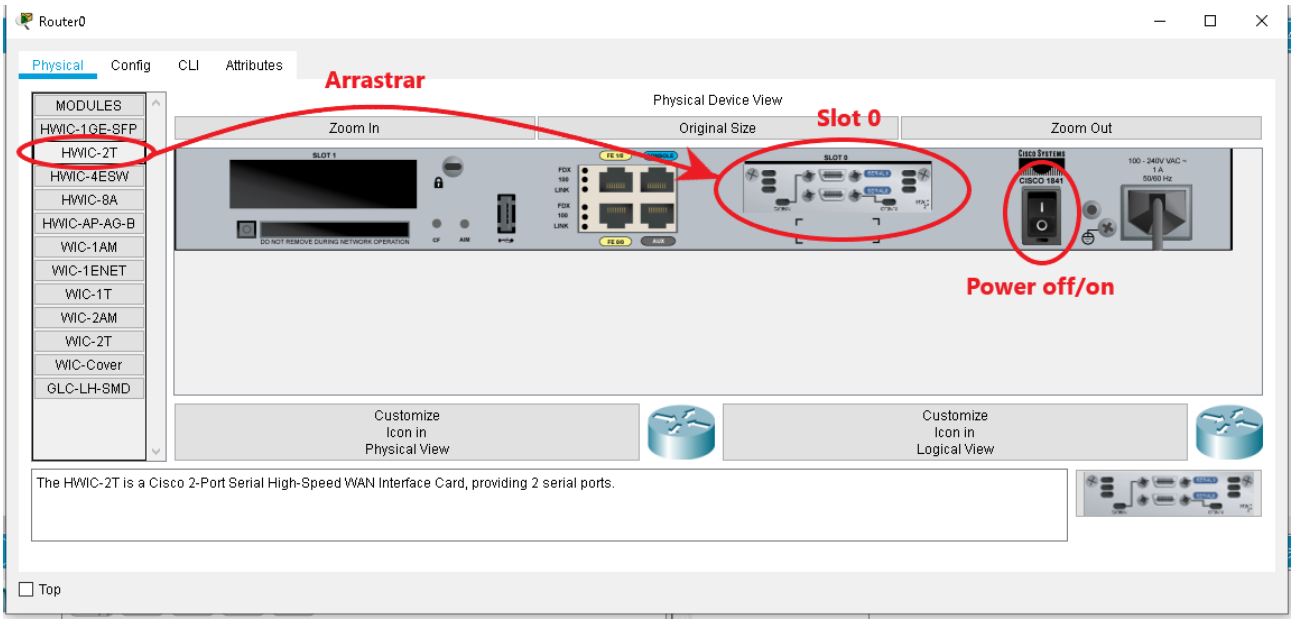


Figura 2. Inserción de tarjeta de interfaces serie en el router.

Una vez esté lista la red, compruebe que todo funciona correctamente y que la red tiene una conectividad total realizando pings entre todos los nodos. Active el servidor HTTP en el servidorWWW y compruebe que se puede acceder a él tanto desde la red externa como desde la interna. Una vez que todo funcione, responda a la siguiente pregunta.

Aquí se incluye una pregunta aleatoria de un banco de preguntas sobre direccionamiento IP y subredes.

10.4 Proteger la red corporativa

La zona de red corporativa alberga los servidores privados y los clientes internos. Ninguna otra red debería poder acceder a ella de manera descontrolada. Efectúa los dos siguientes pasos para proteger esta red corporativa:

Paso A

Configura una lista de acceso extendida para proteger la red corporativa. La protección de una red corporativa empieza por especificar qué tráfico puede salir de la misma. Esto que puede parecer extraño en principio, reduce el daño producido por los empleados *hackers*. La

primera lista de acceso especifica qué tráfico puede salir de la red interna, o lo que es lo mismo, qué tráfico puede entrar al Router por la interfaz Fa0/1.

Entra en la pestaña CLI del Router y asegúrate de que estás en el nivel inicial (tiene que aparecer "Press RETURN to get started"). Si no es así, ejecuta el comando exit hasta que llegues al nivel inicial.

A continuación indica al Router la siguiente secuencia de órdenes:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# access-list 101 permit ip 192.168.10.0 0.0.0.255 any
Router(config)# access-list 101 deny ip any any
```

El primer comando activa el modo privilegiado, que permite ejecutar comandos avanzados. El segundo comando entra en el modo de configuración. Más tarde se puede salir del modo de configuración ejecutando 'exit' repetidas veces o pulsando 'control + z'.

La primera línea de configuración define la lista de acceso 101 que sólo permitirá tráfico IP procedente de los usuarios corporativos válidos en la red 192.168.10.0. La segunda línea de configuración realmente no es necesaria debido al **deny all** implícito en toda lista de acceso, pero mejora la legibilidad del código.

Pasemos a aplicar la lista de acceso al tráfico entrante de la interfaz de red corporativa (interna) del Router. Introduce las siguientes operaciones:

```
Router(config)# interface fastEthernet 0/1
Router(config-if)# ip access-group 101 in
```

Prueba las listas de acceso haciendo ping a todos los sistemas y routers desde cada host. Todos los hosts deberían ser capaces de hacer ping a cualquier ubicación.

Paso B

A continuación, configura una lista de acceso extendida para el tráfico que llega a la red interna desde otras redes, que será aquel procedente de internet o de la DMZ. En un primer paso de configuración, vamos a permitir las respuestas a conexiones originadas en la red corporativa.

Introduce la siguiente orden (¡cuidado con el nivel de configuración!):

```
Router(config)# access-list 102 permit tcp any any established
```

La palabra clave established de la línea permite sólo tráfico TCP de respuesta, por tanto respuestas a conexiones originadas en la red corporativa 192.168.10.0/24. Para facilitar la administración de la red y la solución de problemas, deberíamos permitir también tráfico de respuestas a pings solicitados desde la red corporativa, por tanto respuestas ICMP originadas en la red interna.

Introduce los siguientes comandos:

```
Router(config)# access-list 102 permit icmp any any echo-reply
Router(config)# access-list 102 permit icmp any any unreachable
```

La primera línea permite el paso de los pings que han sido correctos, mientras que la segunda se lo permite a los que no han alcanzado la IP de destino del ping. Por el momento no deseamos que pase ningún tráfico más a la red corporativa, por lo que cerramos esa posibilidad.

Teclea la siguiente orden:

```
Router(config)# access-list 102 deny ip any any
```

Aplica la lista de acceso a la interfaz de Router de la red interna en sentido saliente (desde el punto de vista del router) con las siguientes líneas:

```
Router(config)# interface fastEthernet 0/1
Router(config-if)# ip access-group 102 out
```

Recuerda que una interfaz puede soportar solamente una lista de acceso entrante y otra saliente por protocolo. Sal del modo configuración (exit hasta que aparezca el prompt Router#, o alternativamente, control+z). Utiliza la orden **show access-lists** para comprobar la sintaxis de las listas de acceso construidas y aplicadas. La salida debería parecerse a la siguiente (excepto quizás en la cuenta del número de veces que se ha aplicado cada regla, *matches*):

```
Router# show access-lists
Extended IP access list 101
        permit ip 192.168.10.0 0.0.0.255 any (2 match(es))
        deny ip any any
Extended IP access list 102
        permit tcp any any established
        permit icmp any any echo-reply
        permit icmp any any unreachable
        deny ip any any
```

Puedes también verificar que las ACL han sido aplicadas correctamente a la interfaz con el comando **show ip interface <interface>**:

```
Router# show ip interface fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  (...)
  Outgoing access list is 102
  Inbound access list is 101
  (...)
```

Puede que tengas que borrar y volver a escribir las listas de acceso si observas algún error. Si es así, entra en el modo configuración y en la interfaz correspondiente, y usa la orden **no ip access-group <nº ACL> <in/out>** para eliminar la asignación de la lista de acceso a la interfaz. A continuación, modifica la lista de acceso (debes eliminarla con el comando 'no access-list <nº ACL>'), y vuelve a asignarla a la interfaz.

El siguiente comando refleja un **hipotético** caso de borrado de la lista 102 (EN NUESTRO CASO **NO** QUEREMOS BORRARLA, por lo que **NO LO HAGAS**):

```
Router(config)# interface fastEthernet 0/1
Router(config-if)# no ip access-group 102 out
```

Ahora debe verificar el correcto funcionamiento de las listas de acceso haciendo ping entre todos los nodos de la red. Recuerde que el primer ping que realice entre dos dispositivos

puede que un router lo descarte, por lo que repita varias veces cada ping para estar seguro. A continuación, responda las siguientes preguntas.

> Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren estudiar el funcionamiento de los filtros aplicados

10.5 Proteger la DMZ

La red que conforma la DMZ albergará únicamente un servidor que proporcionará servicios web accesibles desde el exterior. La empresa añadirá más tarde otros servicios, como el correo electrónico, FTP y DNS. Hay que configurar listas de acceso extendidas para asegurar la red DMZ.

Paso 1.

Configura una lista de acceso extendida para proteger la red DMZ del tráfico no deseado, del mismo modo que se hizo con la red interna.

Especifica el tráfico que puede salir de dicha red mediante las siguientes órdenes, en modo configuración:

```
Router(config)# access-list 111 permit ip 192.168.1.0 0.0.0.255 any
Router(config)# access-list 111 deny ip any any
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip access-group 111 in
```

Comprueba la lista de acceso recién aplicada, mandando pings desde todos los nodos de la red hacia la red DMZ y viceversa. La configuración actual trabaja al mismo tiempo que la configuración que asegura la red interna. Ten esto en cuenta a la hora de realizar esta comprobación.

El host PCInterno debería poder hacer ping a todas las ubicaciones, sin embargo, ningún host podrá hacer ping al PCInterno.

Paso 2.

A continuación hay que permitir que el tráfico externo correcto entre en la red DMZ. En concreto, este tráfico serán las peticiones HTTP al servidor web.

Introduce lo siguiente:

```
Router(config)# access-list 112 permit tcp any host 192.168.1.10 eq
www
```

(el último parámetro indica el puerto TCP para el protocolo HTTP, que es el 80, aunque en equipos CISCO esto se puede indicar de forma numérica, o también con el nombre del protocolo, en el caso de HTTP, con "www").

Por razones de administración, sería útil permitir que los usuarios de la red interna pudieran hacer ping al servidor web. Los usuarios externos no deberían poder hacerlo. Añadiremos una línea a la lista de control de acceso iniciada antes:

```
Router(config)# access-list 112 permit icmp 192.168.10.0 0.0.0.255
host 192.168.1.10
```

Para finalizar la lista, introducimos la línea de denegación por defecto:

```
Router(config)# access-list 112 deny ip any any
```

Una vez finalizada la lista, la aplicamos a la interfaz correspondiente en el sentido saliente (desde el punto de vista del router, ya que lo que queremos hacer es aplicar el filtro al tráfico que sale por la interfaz Fa0/0 hacia la red DMZ, que es la red donde está el servidor web):

```
Router(config)# interface fastEthernet 0/0
Router(config-if)# ip access-group 112 out
```

Ya tenemos la red DMZ (y la interna) configurada. Para comprobar las listas de acceso puede utilizar el comando **show access-lists**. El resultado debería parecerse al siguiente:

```
Router# show access-lists
Extended IP access list 101
      permit ip 192.168.10.0 0.0.0.255 any (73 match(es))
      deny ip any any
Extended IP access list 102
      permit tcp any any established (18 match(es))
      permit icmp any any echo-reply (4 match(es))
      permit icmp any any unreachable
      deny ip any any (3 match(es))
Extended IP access list 111
      permit ip 192.168.1.0 0.0.0.255 any (28 match(es))
      deny ip any any
Extended IP access list 112
      permit tcp any host 192.168.1.10 eq www (30 match(es))
      permit icmp 192.168.10.0 0.0.0.255 host 192.168.1.10 (2
match(es))
      deny ip any any (38 match(es))
```

Puede que tengas que borrar alguna lista de control de acceso si observas alguna discrepancia. Prueba las listas de control de acceso verificando las comunicaciones ping y http. Ten en cuenta que ambos hosts deberían poder acceder a la página web de servidor web. Realiza las operaciones oportunas para conseguir el correcto funcionamiento de la red y poder responder a la siguiente pregunta.

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren estudiar el funcionamiento de los filtros aplicados

10.6 Disuasión del spoofing

Una de las técnicas más comunes de ataque realizadas consiste en falsificar una dirección IP origen válida, una práctica que se conoce como *spoofing*. Este tipo de ataques persigue inundar la red con tráfico de difusión introduciendo una gran cantidad de paquetes en la red que provocan respuestas masivas a una dirección interna válida. En ocasiones el objeto de este spoofing es puramente anular el funcionamiento de la red o de un host, pero a menudo el atacante también puede pretender interceptar y manipular el tráfico IP entre dos o más sistemas informáticos.

Para intentar defenderse de este tipo de ataques, se comprueba que todo paquete entrante tenga una dirección IP de origen externa. En este caso configuraremos una lista de acceso para que los hosts de Internet no puedan falsificar fácilmente una dirección de la red interna.

Las dos direcciones IP que los hackers intentan falsificar más frecuentemente son las direcciones internas válidas (por ejemplo 192.168.10.20) y las direcciones de *loopback* (por ejemplo 127.0.0.1). (NOTA: Las direcciones de loopback son utilizadas por los nodos para comunicarse consigo mismos, aún en ausencia de red.)

Paso 1.

Configura tu lista de control de acceso entrante que dificulte a los usuarios exteriores introducir paquetes con direcciones IP origen falsificadas y aplícala a la interfaz Serial 0/0/0. Para ello introduce las siguientes operaciones:

```
Router(config)# access-list 121 deny ip 192.168.10.0 0.0.0.255 any
Router(config)# access-list 121 deny ip 127.0.0.0 0.255.255.255 any
Router(config)# access-list 121 permit ip any any
Router(config)# interface serial 0/0/0
Router(config-if)# ip access-group 121 in
```

Verifica la sintáxis de las listas de acceso de Router con el comando **show ip access-lists**. Debería aparecer una respuesta similar a la siguiente:

```
Router# show ip access-lists
Extended IP access list 101
      permit ip 192.168.10.0 0.0.0.255 any (82 match(es))
      deny ip any any
Extended IP access list 102
      permit tcp any any established (21 match(es))
      permit icmp any any echo-reply (7 match(es))
      permit icmp any any unreachable
      deny ip any any (8 match(es))
Extended IP access list 111
      permit ip 192.168.1.0 0.0.0.255 any (46 match(es))
      deny ip any any
Extended IP access list 112
      permit tcp any host 192.168.1.10 eq www (41 match(es))
      permit icmp 192.168.10.0 0.0.0.255 host 192.168.1.10 (4
match(es))
      deny ip any any (46 match(es))
Extended IP access list 121
      deny ip 192.168.10.0 0.0.0.255 any
      deny ip 127.0.0.0 0.255.255.255 any
      permit ip any any (20 match(es))
```

Observa que junto a cada regla aparece el número de paquetes que, al concordar con la expresión (*match*), se les ha aplicado el permiso o la denegación. Compruebe que esta lista no ha modificado el comportamiento anterior de la red. Efectúa varios pings y accesos http para comprobar que es así, y una vez hayas comprobado que la red funciona conforme a nuestras necesidades, trata de responder a la pregunta de la siguiente página.

Aquí se incluyen varias preguntas aleatorias de sendos bancos de preguntas que requieren estudiar el funcionamiento de los filtros aplicados

10.7 Proxy web (si es que llegas hasta aquí)

[*Nota: Este último ejercicio no tiene asociada una pregunta de comprobación y es opcional, pero aun así sigue siendo interesante.*]

Plantéate que se deseara *a posteriori* la instalación de un proxy web en la red DMZ, con el fin de que filtrara todo el tráfico http desde la red interna al exterior. Este proxy estará instalado

en el host "servidorWWW". Así, la entidad podría garantizar el que los empleados accedan exclusivamente a las webs que fueran útiles para su trabajo. Como podrás suponer no es que vayamos a configurar el proxy web en esta lección, pero sí podemos adecuar las listas de control de acceso correspondientes. Las reglas a considerar en este caso se concretan en las siguientes acciones a nivel de rutado:

1. Impedir el paso hacia el ISP de las peticiones http (TCP, puerto 80) originadas en la red interna y con destino a cualquier dirección externa.
2. Permitir el paso de paquetes TCP con destino al puerto 80 del ServidorWWW originados en la red interna.
3. Permitir la salida de peticiones http desde servidorWWW en la red DMZ hacia el exterior, y la entrada de las respuestas correspondientes.

Trata de confeccionar las listas de control de acceso necesarias para implementar el paso obligado por el proxy web. Posteriormente, comprueba que funcionan correctamente añadiendo un servidor web en la red externa e intentando conectarte a él desde un cliente en PCInterno y desde ServidorWWW.

Si has llegado hasta aquí (y lo has hecho bien...) ¡Enhorabuena!