**Práctica 1: Introducción**

**PACKET TRACER**

***Curso 2023 - 2024***

**Introducción a Redes de Computadoras**

Docente: Roberto Olea

DEPARTAMENTO DE INGENIERÍA DE SISTEMAS Y AUTOMÁTICA

**OBJETIVOS DE LA PRÁCTICA**

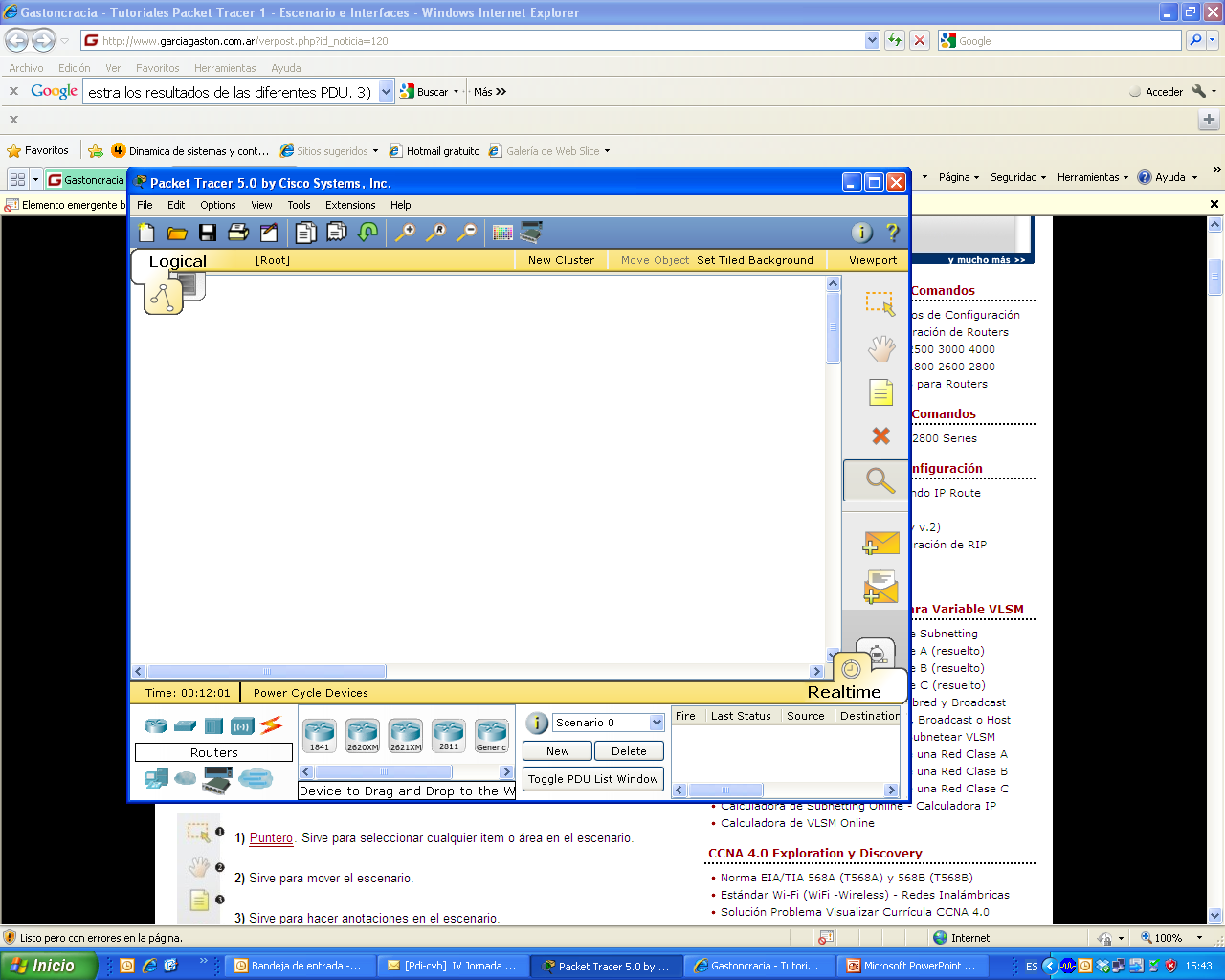
Esta práctica tiene como objetivo introducir al alumno en la herramienta de simulación de redes **Packet** **Tracer**, tanto en su interface gráfica como en las posibilidades que ofrece para el diseño y análisis de una red de computadoras.

**PARTE 1: PRIMEROS PASOS CON PACKET TRACER**

Packet Tracer de Cisco System es un programa de simulación y aprendizaje de redes interactivo. Esta herramienta permite a los usuarios crear topologías de red, configurar los dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Su interfaz gráfico es muy intuitivo permitiendo crear topologías arrastrando dispositivos a la pantalla y entrar en sus consolas de configuración solamente haciendo click en los mismos.

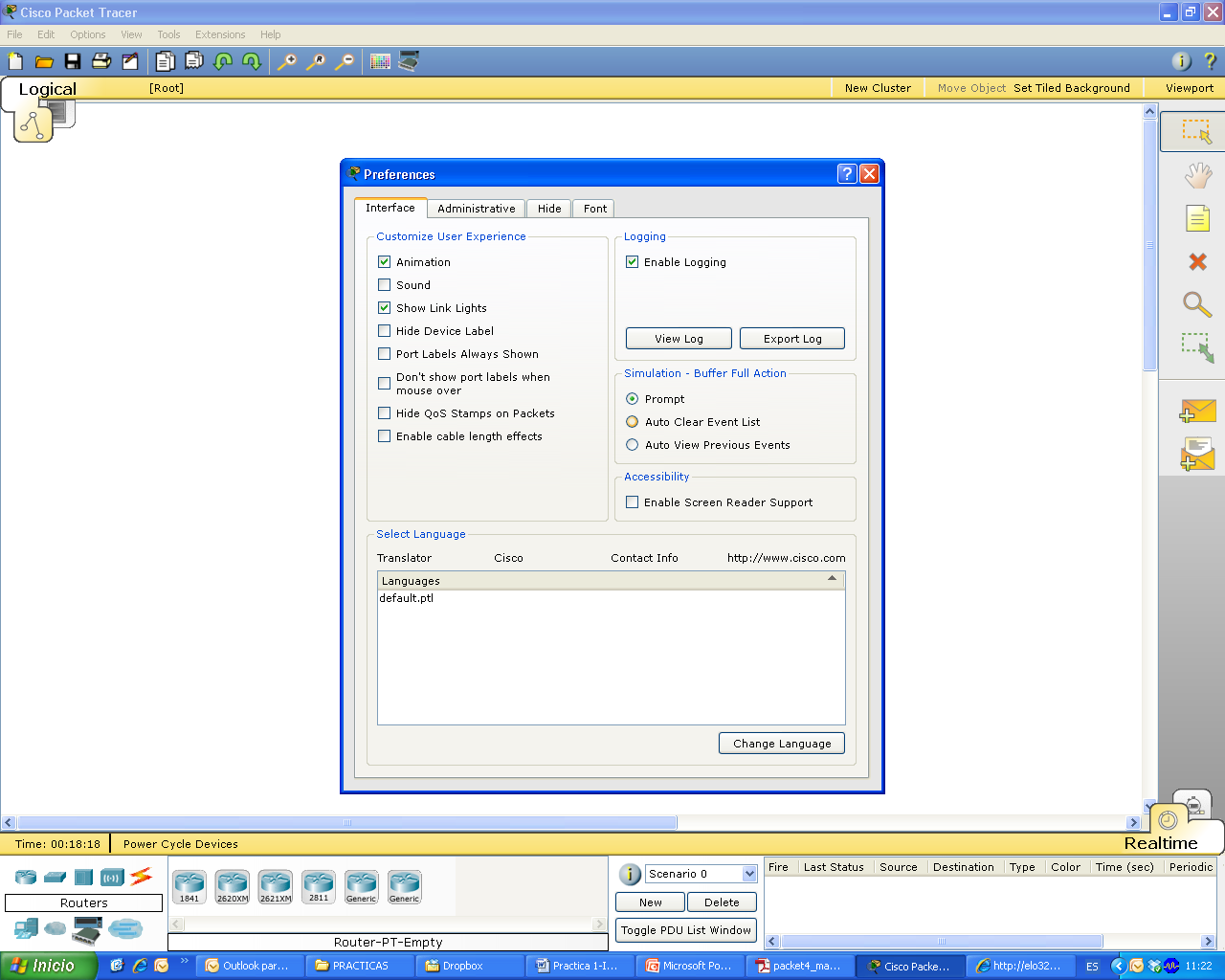
**INTERFAZ GRAFICO**

Al abrir el programa aparece la siguiente pantalla gráfica.



La zona central, **área de trabajo**, es donde se construyen las topologías de red.

Como otras herramientas dispone de **menús principales** FILE, EDIT, OPTIONS, HELP… y dispone de una **barra de acceso rápido** que contiene las opciones para crear un nuevo escenario (NEW), abrir un escenario (OPEN), guardar cambios en un escenario (SAVE), imprimir un escenario (PRINT) y un asistente de actividades (ACTIVITY WIZARD).

En el menú FILE, se encuentran todas las opciones descritas en la barra de acceso rápido y la opción de guardar como (SAVE AS).

En el menú EDIT disponemos de las opciones para copiar, pegar y deshacer.

En el menú OPTIONS, se encuentra la opción PREFERENCES, que permiten personalización la herramienta Packet Tracer.

En VIEW se encuentran las opciones de zoom y de activación de las barras de herramientas.

Dentro del menú TOOL tenemos opciones para dibujar figuras y generar dispositivos personalizados.

La **barra de herramientas** proporciona las herramientas para la manipulación de los dispositivos:

1. - Selección de dispositivos y conexiones, no selecciona conexiones wireless.

2. - Movimiento del escenario o área de trabajo.

3. - Notas, permite agregar notas que ayudan a entender la topología diseñada.

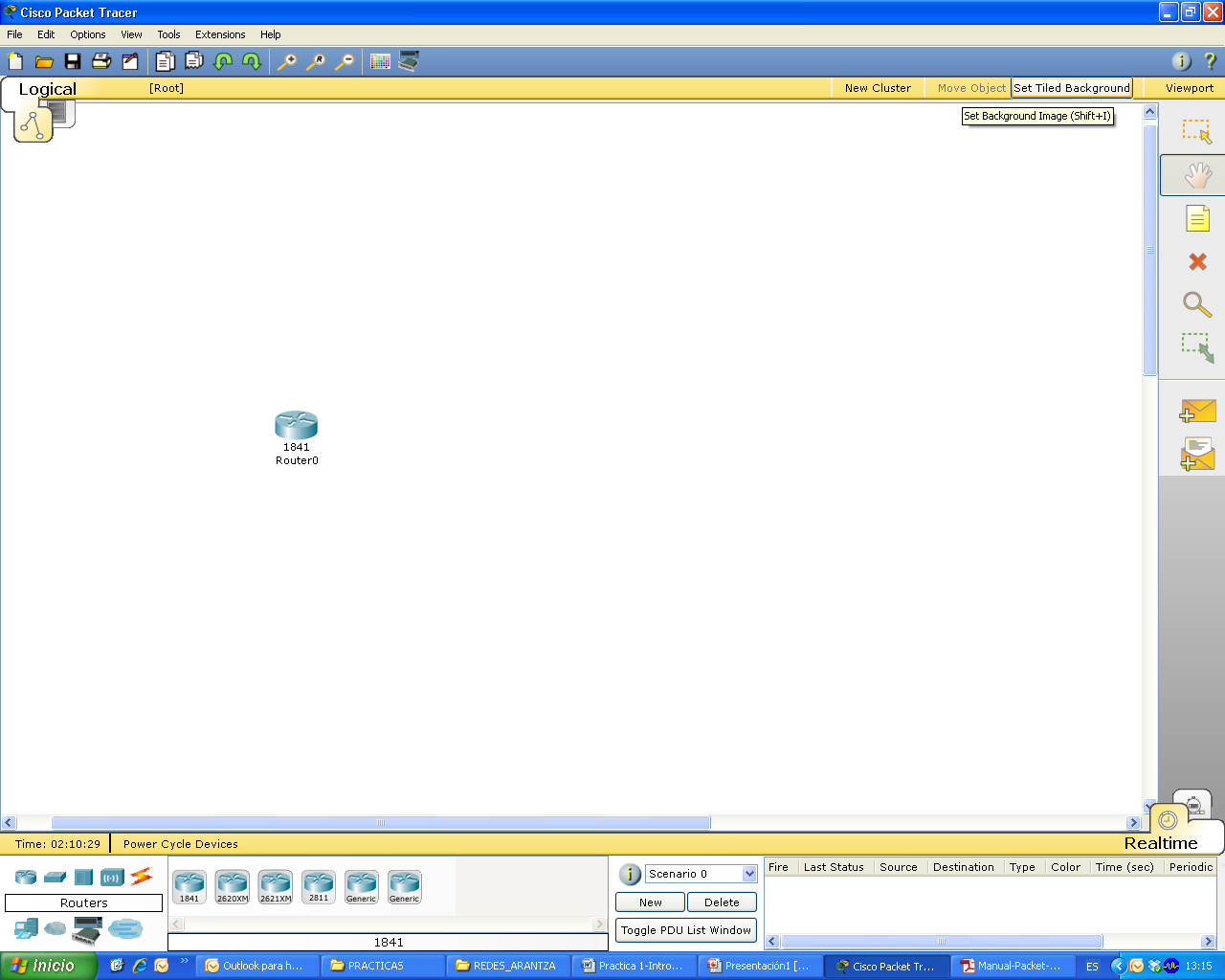
4. - Eliminar, permite eliminar cualquier dispositivo, conexión (excepto wireless) y notas.

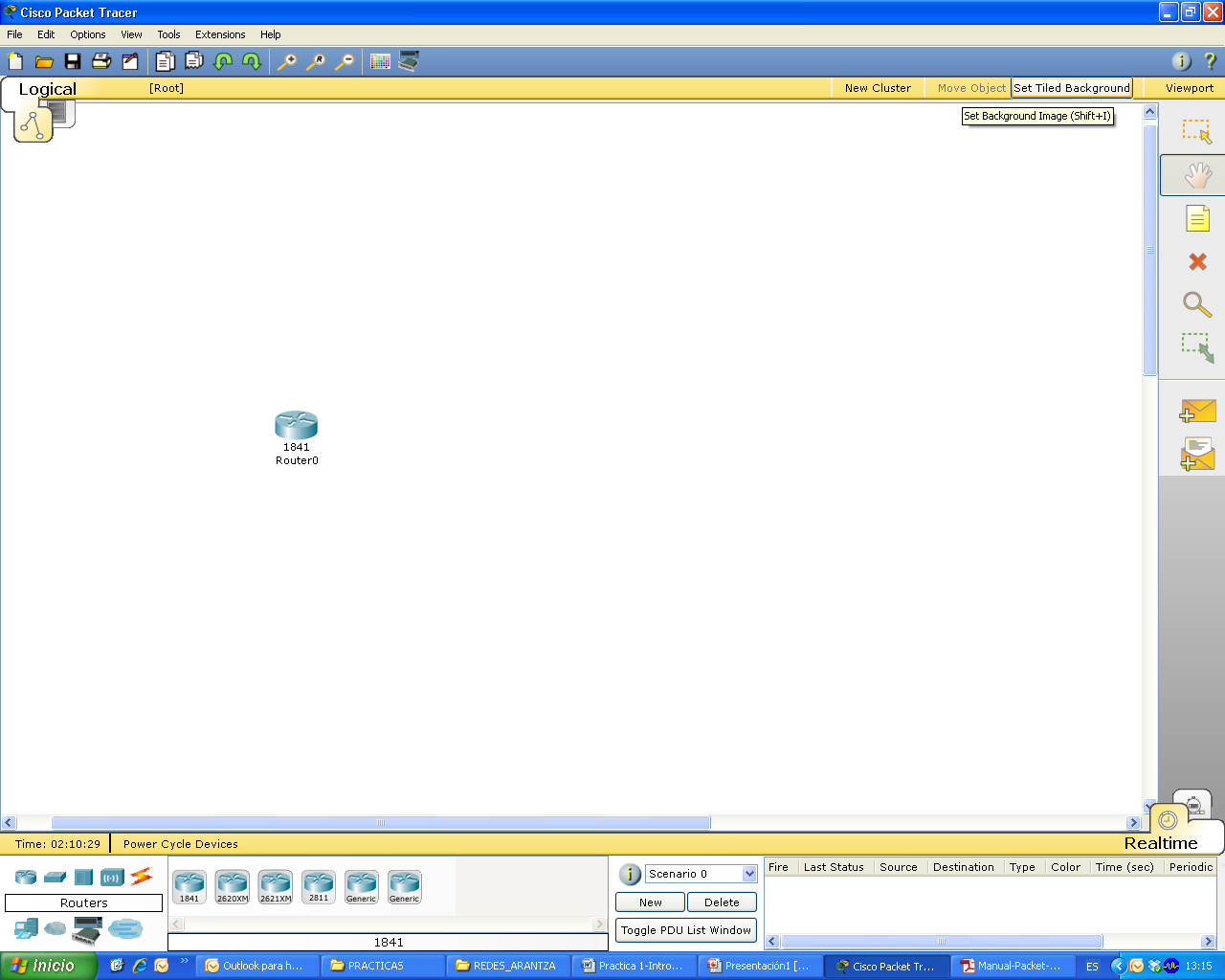
5. - Inspector, permite visualizar la tabla correspondiente al dispositivo seleccionado, entre ellas ARP, MAC y ROUTER.

6. - Mensaje Simple UDP, permite crear paquete del tipo ICMP entre dispositivos.

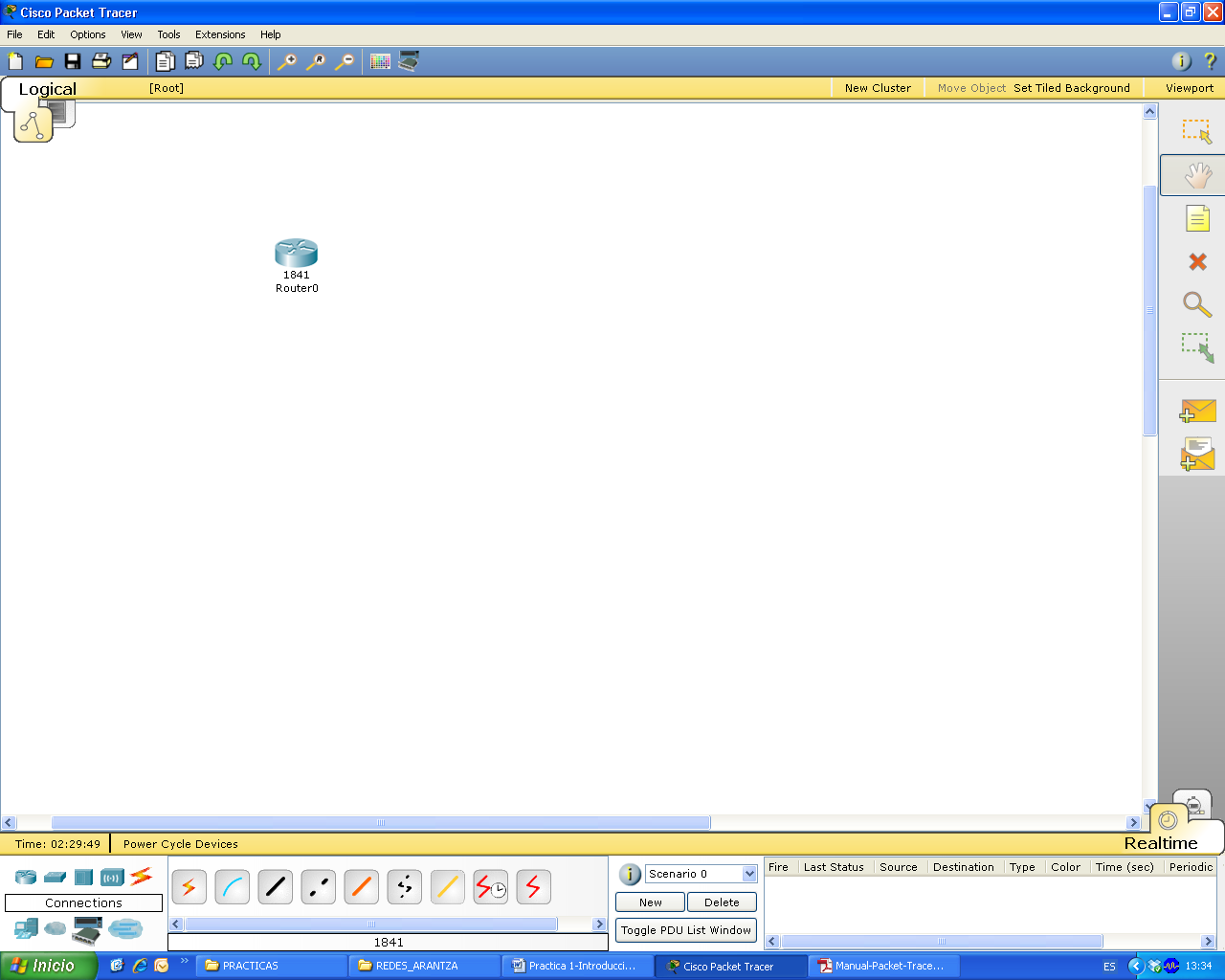
7. - Mensaje Complejos UDP, permite crear paquetes personalizados entre dispositivos.

El **panel de dispositivos** en la parte inferior izquierda de la pantalla se muestra los tipos de dispositivos que pueden ser agregados:routers, switchs, hubs, dispositivos wireless, conexiones, dispositivos finales, emulador de WAN, dispositivos personalizados…





En **el panel de dispositivos seleccionados** se muestran los diferentes dispositivos disponibles para utilizar en la topología. Para introducirlo se hace clic en el dispositivo que deseamos utilizar y luego clic en la parte del escenario donde se colocará el dispositivo.



Dentro de las **conexiones** se encuentran todas las conocidas: punto a punto (Cooper Straight - through), cruzadas (Cooper Cross - over), consola (console), fibra óptica (fiber), teléfono (telephone), Serial DCE y Serial DTE. Existe una conexión que detecta automáticamente el tipo correcto según los dispositivos a conectar.

Hay **dos modos de funcionamiento**, uno es el modo **tiempo real** (REALTIME), en este modo es donde se crean y configuran las topologías de red; y el modo **simulación** (SIMULATION) en el cual se pone a funcionar la red para testear su comportamiento. Para cambiar de un modo a otro en la parte inferior derecha de la pantalla disponemos de dos pestañas. El modo tiempo real es representado por un reloj, y el modo simulación es representado con un cronometro.



El sistema dispone además de **dos vistas**, la **lógica** (LOGICAL) y la **física** (PHYSICAL). En la vista lógica se agregan todos los dispositivos y en la vista física se hace la distribución física real de las redes, distribuida en ciudades, departamentos y oficinas. Las vistas se seleccionan con las pestañas que aparecen en la parte inferior de la barra de acceso rápido.



**AGREGAR Y ELIMINAR DISPOSITIVOS**

Como se mencionó anteriormente, para poder **agregar** un dispositivo, tal como un router, switch, ordenadores, etc.; es necesario únicamente hacer un clic simple sobre el que deseamos y colocarlo en el área de trabajo. Notaremos que al hacer clic sobre el dispositivo el cursor cambia de una flecha a un signo más. Si deseamos colocar más de un dispositivo del mismo tipo únicamente debe presionar la tecla **CTRL** antes de seleccionar el dispositivo, el cursor permanece con el signo más, después de agregar el primero. Una vez agregados los dispositivos para terminar se pulsa la tecla **ESC**, o se hace un clic sobre el botón del dispositivo que selecciono.

Para **eliminar** un dispositivo, se seleccionarlo y luego en la barra herramientas comunes se hace clic en el botón identificado con una equis. Otra forma de eliminar un dispositivo es con la tecla DEL. También se pueden seleccionar un grupo de dispositivos, y repetir cualquier de los dos pasos mencionados anteriormente.

***Practica*** *a añadir y eliminar dispositivos.*

**INFORMACIÓN DE ESTADO DE LOS DISPOSITIVOS**

Existen dos formas para mostrar la información de los estados de cada uno de los dispositivos, una de ellas es utilizar el inspector (LUPA) de la barra de herramientas comunes, que sirve para visualizar las tablas **ARP** (Address Resolution Protocol), **MAC** y **ROUTING**. El cursor tendrá la apariencia de una lupa, entonces se selecciona con un clic simple el dispositivo y se le selecciona el tipo de tabla, desplegándose un cuadro de texto con la información solicitad.

La segunda forma es posicionar el cursor sobre el dispositivo y esperar que se despliegue la información, la cual desaparecerá una vez que el usuario saque el mouse del dispositivo.

**CONFIGURACIÓN DE EQUIPOS**

Haciendo clic con el botón izquierdo del mouse en cada dispositivo que encuentre en el área de trabajo se puede ver, definir y modificar la configuración de los dispositivos.

Dependiendo del tipo de dispositivo aparece una ventana con un número de pestañas diferentes.

Los dispositivos tipo **router** y **switch** tiene tres pestañas

* **Física** (PHYSICAL): muestra los componentes físicos del dispositivo, como los módulos. En esta pestaña, también se pueden agregar nuevos módulos.
* **Configuración** (CONFIG): muestra la información de configuración general, como por ejemplo el nombre del dispositivo.
* **CLI** (IOS COMMAND LINE INTERFACE): permite al usuario configurar el dispositivo con una interfaz de línea de comando.

Los **servidores** y el **hubs** contienen dos pestañas.

* **Física** (PHYSICAL): muestra los componentes del dispositivo, como por ejemplo los puertos. En esta pestaña, también se pueden agregar nuevos módulos**.**
* **Configuración** (CONFIG): muestra información general, como por ejemplo el nombre del dispositivo.

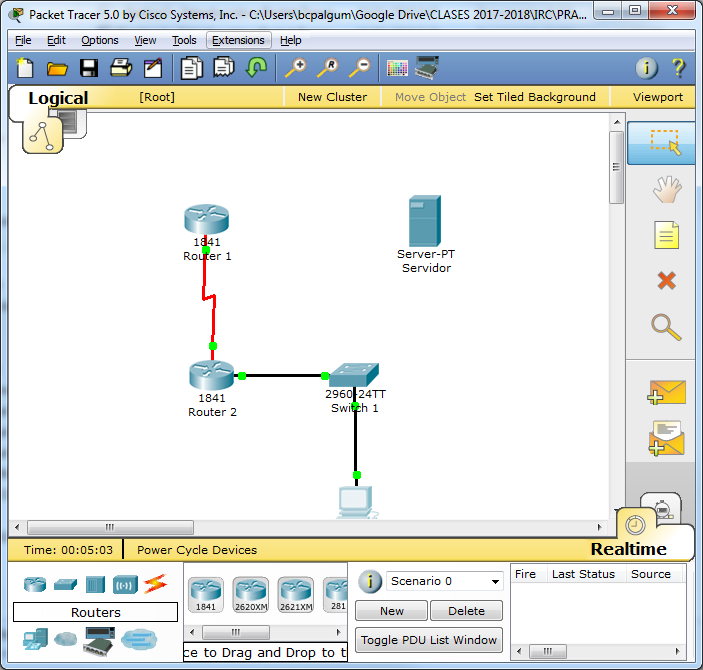
Las **PC** contienen tres pestañas:

* **Física** (PHYSICAL)**:** muestra los componentes del dispositivo. En esta pestaña, también se pueden agregar nuevos módulos.
* **Configuración** (CONFIG): muestra el nombre del dispositivo, la dirección IP, la máscara de subred, el DNS y la información del gateway.
* **Escritorio** (DESTOP): permite al usuario configurar la dirección IP, la máscara de subred, el gateway por defecto, el servidor DNS, dial-up e inalámbrico. Con la pestaña Escritorio también se puede acceder a un emulador de terminal, a la petición de entrada de comandos y a un navegador Web simulado.

**PRACTICA 1.1**

Una vez que se ha realizado una pequeña introducción de Packet Tracer y su entorno gráfico se va a comenzar a trabajar dentro del entorno.

Abrir el fichero de **Packet Tracer** **“*Practica1\_RedBase*”** que se proporciona con el guion de la práctica. La topología de red que se proporciona está formada por dos routers, un servidor y un PC.



Pasos a seguir:

1. **Añadir un elemento**: Introducir un nuevo PC, se denominará PC 2 y un nevo switch (Switch 2).
2. **Conectar dispositivos:** utilizando la conexión automática realizar las siguientes conexiones

Conectar PC 2 al Switch 1

Conectar el Servidor al Router1 a traves de Switch 2

Observa cómo se activan las conexiones.

**Informe: Cuestión 1:** ¿Cuántos dispositivos podemos conectar al switch que se ha seleccionado?

**26 lo ponía en config-**>interface

**Informe: Cuestión 2:** Intenta enviar un mensaje (ICMP) del PC1 al PC2. ¿Que sucede? Mira la información de los PCs.

**Pc2 has no funtional ports, no se puede enviar la informacion**

1. **Configurar** elPC 2, para ello se le debe asignar la **dirección IP** 172.16.1.121 con **máscara de red** 255.255.0.0 y la **puerta enlace o Gateway** 172.16.1.1. Envía de nuevo el mensaje.

**Informe: Cuestión 3:** ¿Qué es la dirección IP, la máscara de red y la puerta de enlace?

1. **Examina la configuración** de los demás dispositivos moviendo el ratón sobre estos

* Un **router** muestra la información de configuración del puerto/interface de red, incluida la dirección IP, el estado y la dirección MAC. **¿Solo uno?**

**No, los dos lo muestran**

* Un **servidor** muestra la dirección IP, la dirección MAC y la información del gateway
* Un **switch** muestra la información de configuración del puerto, incluida la dirección IP, la dirección MAC, el estado del puerto y la participación VLAN.
* Una **PC** muestra la dirección IP, la dirección MAC y la información del gateway.

1. Haz click sobre cada uno de los dispositivos y examina las pantallas de configuración de que disponen.
2. **Revisión de la configuración**. La configuración de red de este laboratorio consta de dos routers, un switch, un servidor y dos PC. Cada uno de estos dispositivos está configurado previamente o lo has configurado al realizar la práctica. Con todos los conocimientos que tienes hasta ahora debe tratar de rellenar la siguiente tabla.

**Informe: Cuestión 4:** Rellenar la siguiente tabla.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Mascara de subred | Gateway por defecto |
| Router 1 | FaEth0/0 | 192.168.254.1 | 255.255.255.0 | N/A |
| Serial0/ 1/0 | 10.10.10.5 | 255.255.255.252 |
| Router 2 | FaEth0/0 | 172.16.1.1 | 255.255.0.0 | N/A |
| Serial0/ 1/0 | 10.10.10.6 | 255.255.255.252 |
| PC 1 | NIC  Se llama así porq solo hay una | 172.16.1.120 | 255.255.0.0 | 172.16.1.1 |
| PC 2 | NIC | 172.16.1.121 | 255.255.0.0 | 172.16.1.1 |
| Servidor | NIC | 192.168.254.54 | 255.255.255.0 | 192.168.254.1 |

1. **Ayuda de Packet Tracer.** Es bueno recordar que se dispone de una ayuda, útil siempre en los primeros momentos.

**PARTE 2: MODO SIMULACION**

Packet Tracer, como ya se ha comentado dispone de dos modos de funcionamiento el modo de tiempo y el modo simulación. En el **modo tiempo** real podemos ver mensajes a la velocidad a la que usualmente ocurren en el mundo real. En el **modo de simulación**, la intención es ver con el mayor detalle posible cómo se desarrolla una transferencia de datos. Se ven los paquetes pasar por cada nodo de la red, se listan y en cada uno de ellos se puede ver qué transformaciones sufre el paquete y qué decisiones toman los dispositivos en cada capa del modelo OSI, incluso es posible ver de manera simbólica los encabezados de los protocolos en uso.

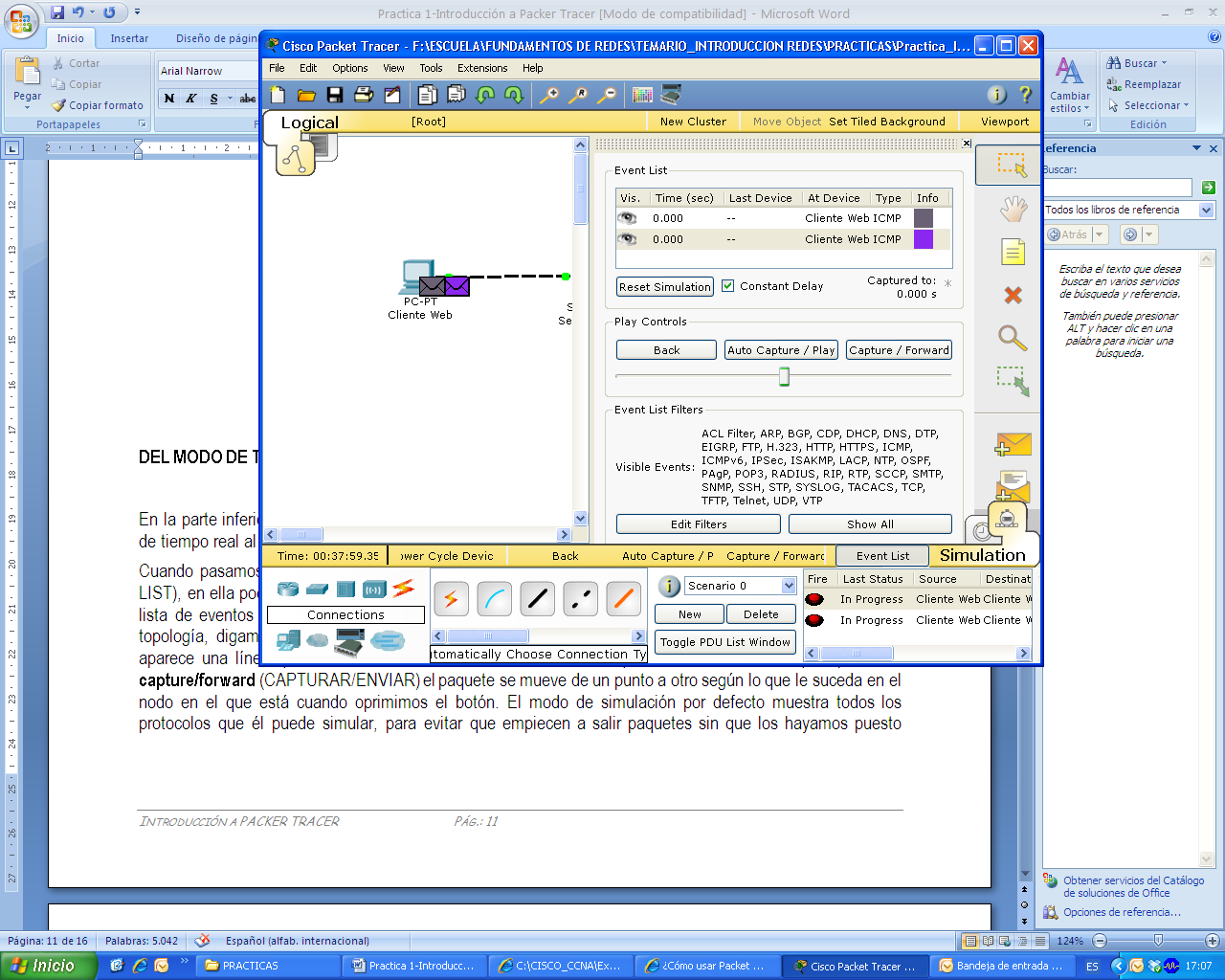
En la parte inferior derecha más lejana de la interfaz de Packet Tracer se encuentra el conmutador para pasar del modo de tiempo real al modo de simulación.

Cuando pasamos al modo de simulación, aparece una ventana adicional llamada **lista de eventos** (EVENT LIST), en ella podemos ver cada paso de todo el proceso de comunicación de nodo a nodo. Cada línea de la lista de eventos es un paso de un paquete por un nodo de la red. Cuando se dispara algún tráfico en la topología el paquete aparece en la topología como un sobre y en la lista de eventos aparece una línea que termina en un cuadrado del mismo color que el sobre.

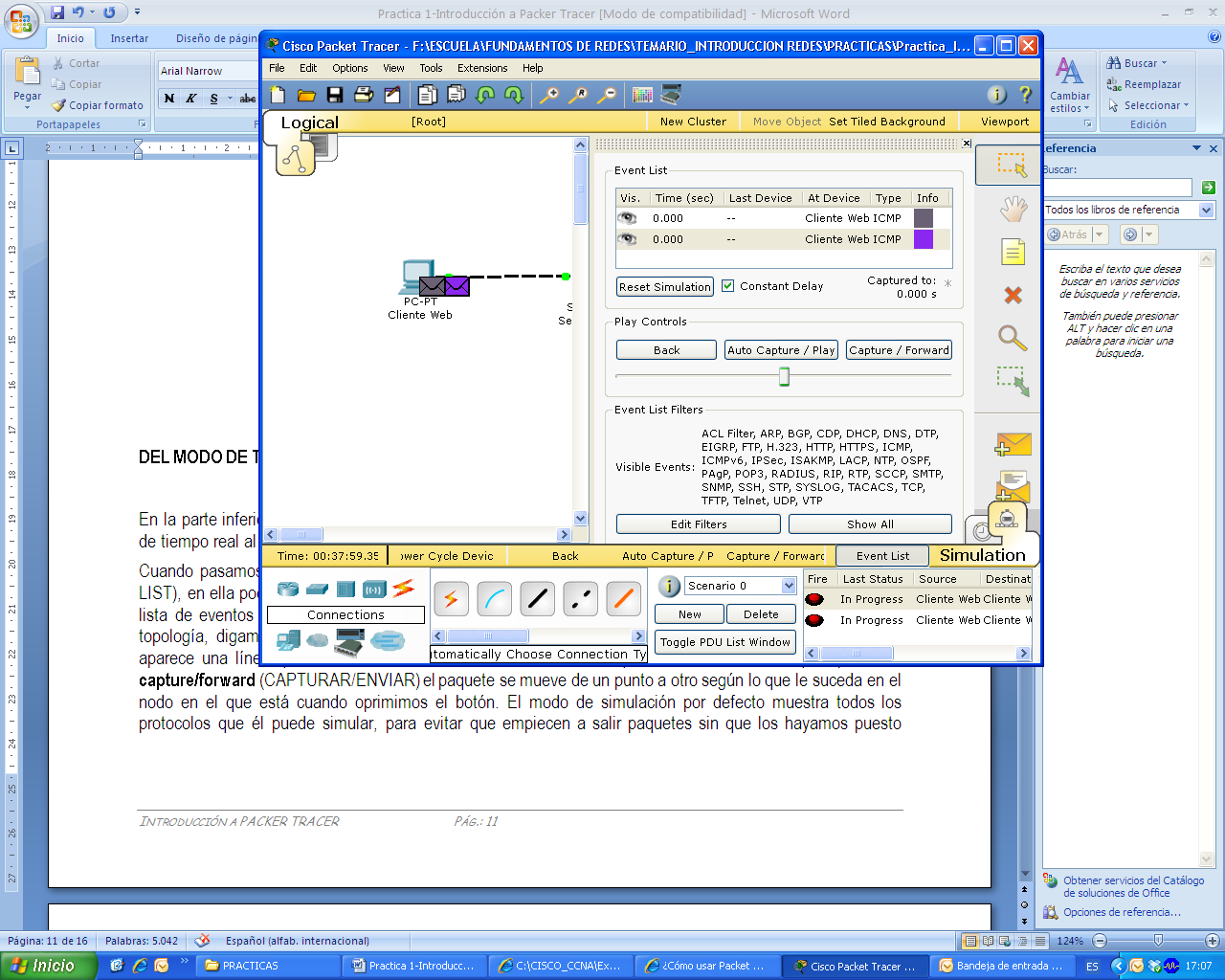
Cada vez que oprimimos **capturar y enviar** (CAPTURE/FORWARD) el paquete se mueve de un punto a otro según lo que le suceda en el nodo en el que está cuando oprimimos el botón.

El modo de simulación por defecto muestra todos los protocolos que él puede simular, para una mejor visualización debemos filtrar el tráfico y dejar sólo el que nos interesa. Para ello utilizaremos **Edit Filters**.

En esta práctica vamos a lanzar un comando **ping** desde el **PC 1** al **PC 2,** este comando utiliza el protocolo ICMP (Internet Control Message Protocol). Dejaremos ver solo el trafico ICMP.



La simulación puede correr paso a paso o automáticamente, cuando usamos CAPTURE/FORWARD nosotros controlamos la simulación, cuando oprimimos AUTO CAPTURE / PLAY la simulación se ejecuta automáticamente y nosotros la podemos detener volviendo a oprimir auto CAPTURE/PLAY.



La velocidad con la que suceden los eventos en el modo de simulación se controla con el indicador que hay justo debajo de los botones de control (BACK, AUTO CAPTURE/PLAY, CAPTURE/FORWARD).

La gran utilidad de este modo no sólo es ver cómo se mueven los paquetes por la topología. El cuadrado de colores y el sobre que se mueve por la topología nos permiten acceder a los detalles de recepción y envío de paquetes en un nodo en particular. Si observan las columnas de la lista de eventos, verán que cada línea indica un nodo y una dirección de tránsito del paquete (At Device, Last Device). Cuando se hacemos clic en el **cuadrado de color** o en el sobre, podemos ver los procesos y decisiones que se hicieron sobre el paquete al entrar y al salir del nodo en particular. Para cada capa del modelo OSI hay una descripción de esos procesos, por ejemplo, si el dispositivo es un enrutador, éste des-encapsula el paquete en capa 2 y lo compara con su tabla de direcciones de capa 2, si el paquete coincide con su dirección de capa 2 lo des-encapsula y lo pasa a la siguiente capa, en capa 3 lo compara con su tabla de enrutamiento y si encuentra una salida lo pasa al proceso de capa 3 de salida y así sucesivamente.

**PRACTICA 1.2**

Para ver cómo funciona el modo simulación de Packet Tracer vamos a **enviar un comando ping desde el PC1 al PC2**.

**PING (¿HOLA ESTAS EN LA RED?)**

PING es una utilidad de diagnóstico en redes de ordenadores que comprueba el estado de conexión de un host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de **paquetes ICMP** de solicitud y respuesta

El comando Ping trabaja en la capa de red del protocolo TCP/IP. El funcionamiento de Ping y del protocolo ICMP, en general, están definidos en [RFC](http://es.wikipedia.org/wiki/Request_For_Comments) 792.

El protocolo IP encapsula el mensaje ICMP dentro de un paquete y lo envía. Suele llamarse Paquete ICMP. En el paquete pueden distinguirse dos conjuntos de datos: La cabecera IP, que contiene los datos estándar de la [Capa de red](http://es.wikipedia.org/wiki/Nivel_de_red), y el **sub-paquete ICMP**, que contiene los datos de control del protocolo. En la **cabecera IP** se especifican el **protocolo** como 0x1 (valor que corresponde al protocolo ICMP) y **tipo de servicio** como 0 (rutinario). En el **sub-paquete ICMP** se especifican los valores:

* **Tipo de mensaje** ICMP: 0x8 en una solicitud (echo) o 0x0 respuesta (echo replay) y
* **Código** a 0x0 si no existe ningún error tanto para la solicitud como respuesta.

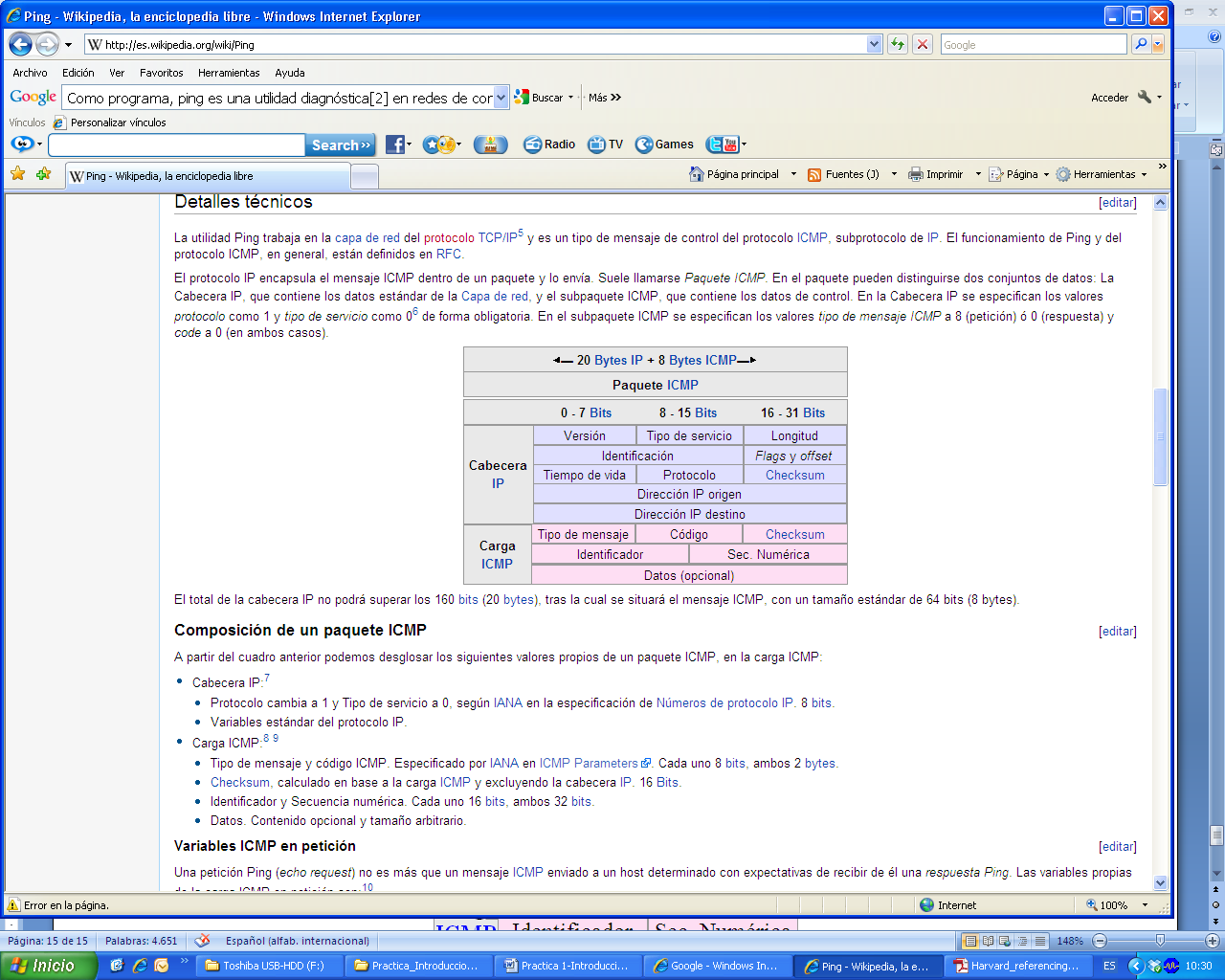


Figura 1.- Formato del mensaje ICMP

El tamaño total de la cabecera IP es de 160 [bits](http://es.wikipedia.org/wiki/Bit) (20 [bytes](http://es.wikipedia.org/wiki/Byte)), tras la cual se situará el mensaje ICMP, con un tamaño estándar de 64 bits (8 bytes).

*(Buscar más información si la necesitáis)*

1. En modo tiempo real vamos a enviar un ping. Para ello, abrir la ficha del ordenador PC 1, dentro del escritorio (*desktop*) abre una ventana de comandos (*comand prompt*) y comprueba con el comando **ping** al PC2 si está conectado. Necesitas conocer la dirección IP del PC2.

**Informe: Cuestión 5:** ¿Qué sucede? ¿Que aparece en la ventana de comandos?

Texto

Descripción generada automáticamente con confianza baja

1. Pasa al modo simulación y ejecuta de nuevo el comando ping, captura solo los paquetes del protocolo ICMP.

**Informe: Cuestión 6:** Realiza un diagrama con los mensajes ICMP que se envían entre los dos PCs. Fíjate en los campos código y número de secuencia.

Sale en event list, por ejemplo: pc1🡪switch1->pc2….

1. Investiga que niveles OSI participan en el envió de estos mensajes (selecciona el cuadrado de color de uno de los mensajes). ¿Que son los niveles OSI?
2. Fíjate en el formato de los mensajes (PDU details) y relaciona con el formato de la figura 1.

**Informe: Cuestión 7:** ¿Cuál es el número de protocolo ICMP? ¿y el tiempo de vida? ¿Qué significado crees que puede tener el número de secuencia en el sub-paquete ICMP?

**0x1.**

1. Intenta conectarte con un **ping** desde el PC 1 con el servidor.

**Informe: Cuestión 8:** ¿Qué sucede? ¿Hasta qué dispositivo llegan los mensajes? ¿Cuál crees que puede ser el motivo? Pista: Analiza la *Routing Table* del Route 1 y 2

Hay que hacerlo poniendo ping y la ip del servidor dentro del pc1. En simulation. Se queda en el router2

En el router2 no pone nada en Next Hop IP, ese puede ser el motivo por el que no le llegan los mensajes.

|  |
| --- |
|  |