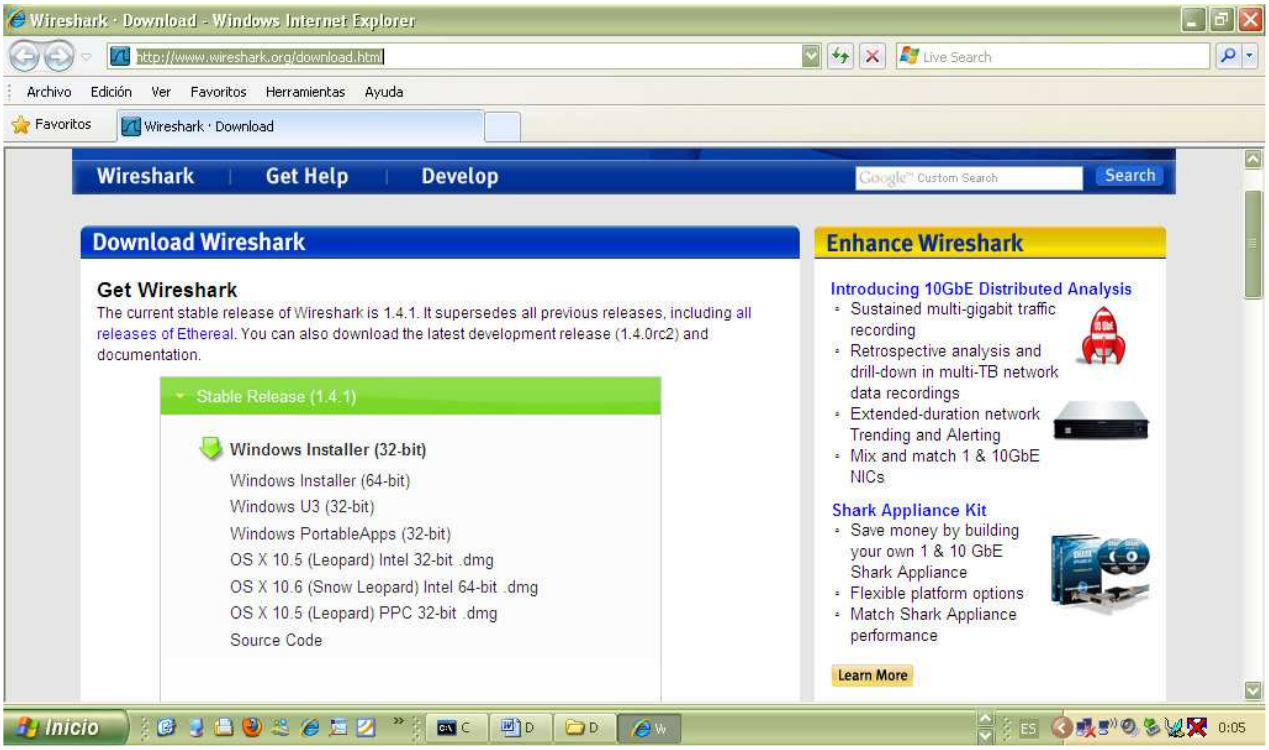
FRANCISCO ANTONIO BELDA DIAZ

PRACTICA 13

Parte 1: WIRESHARK
Parte 2: Ejercicio 7.5.2 de CISCO

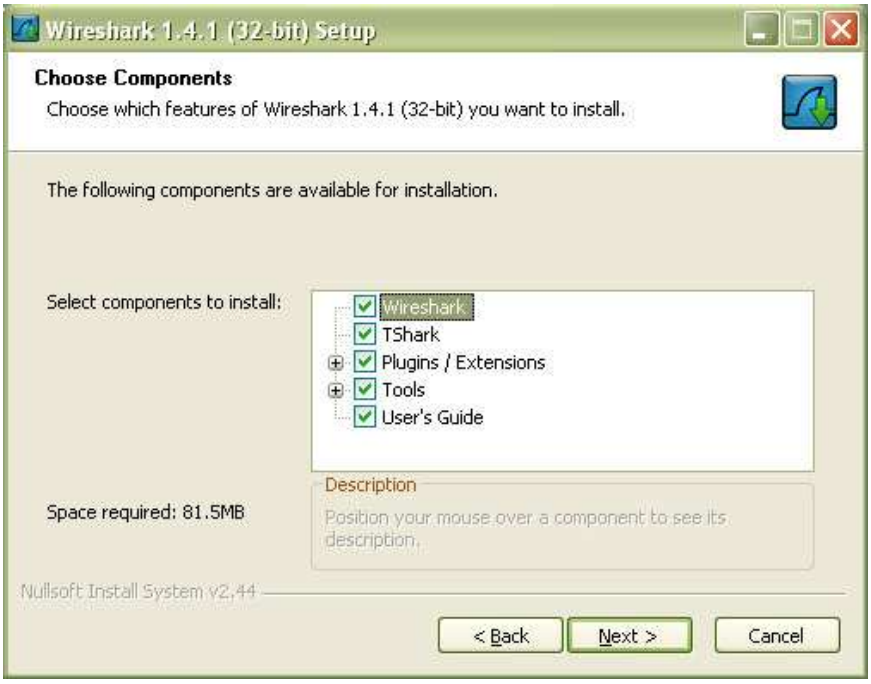
Parte 1: WIRESHARK

Accedemos a la web de descarga de WIRESHARK



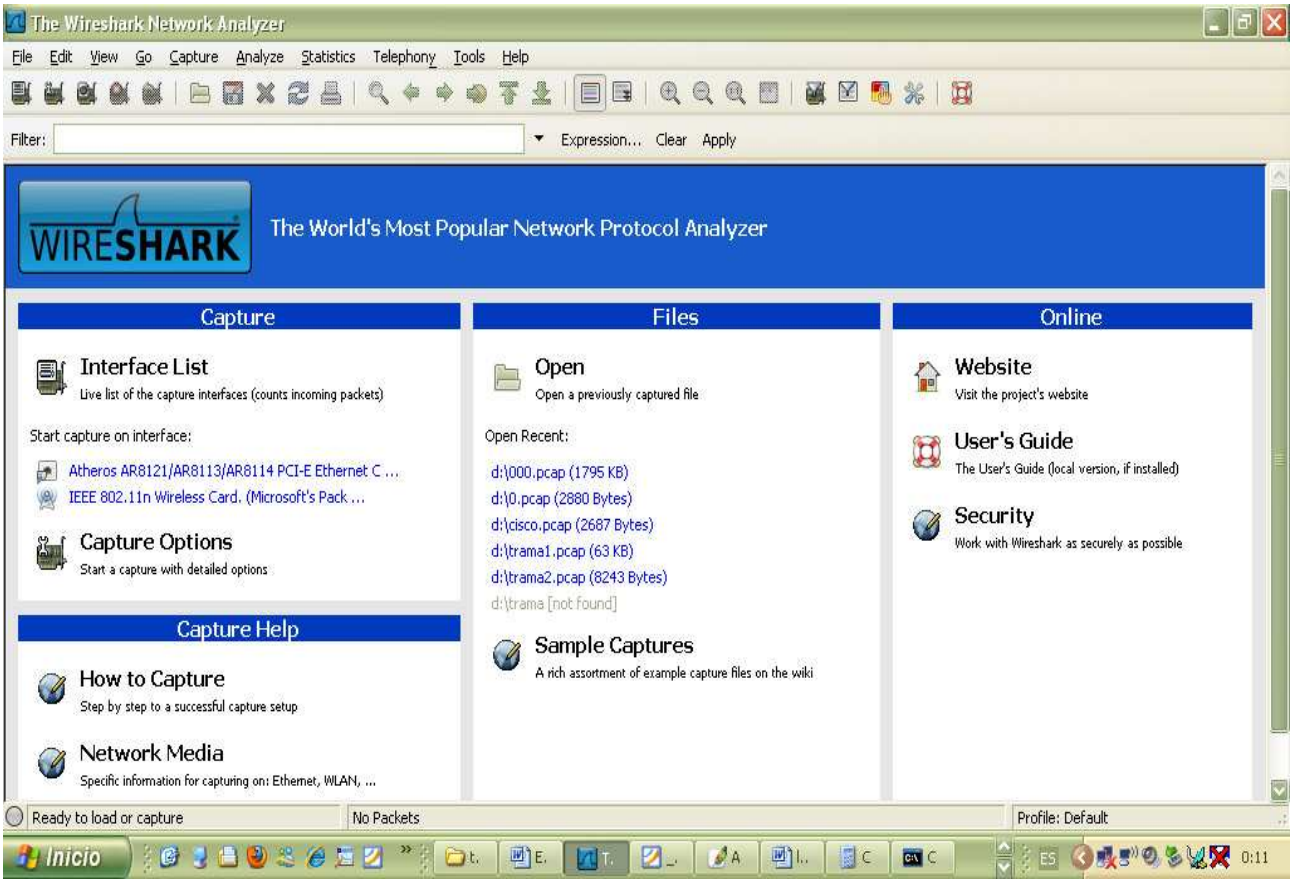
Y descargamos el programa Y a continuación lo instalamos

Seguimos todos los pasos de la instalación, como indica el manual

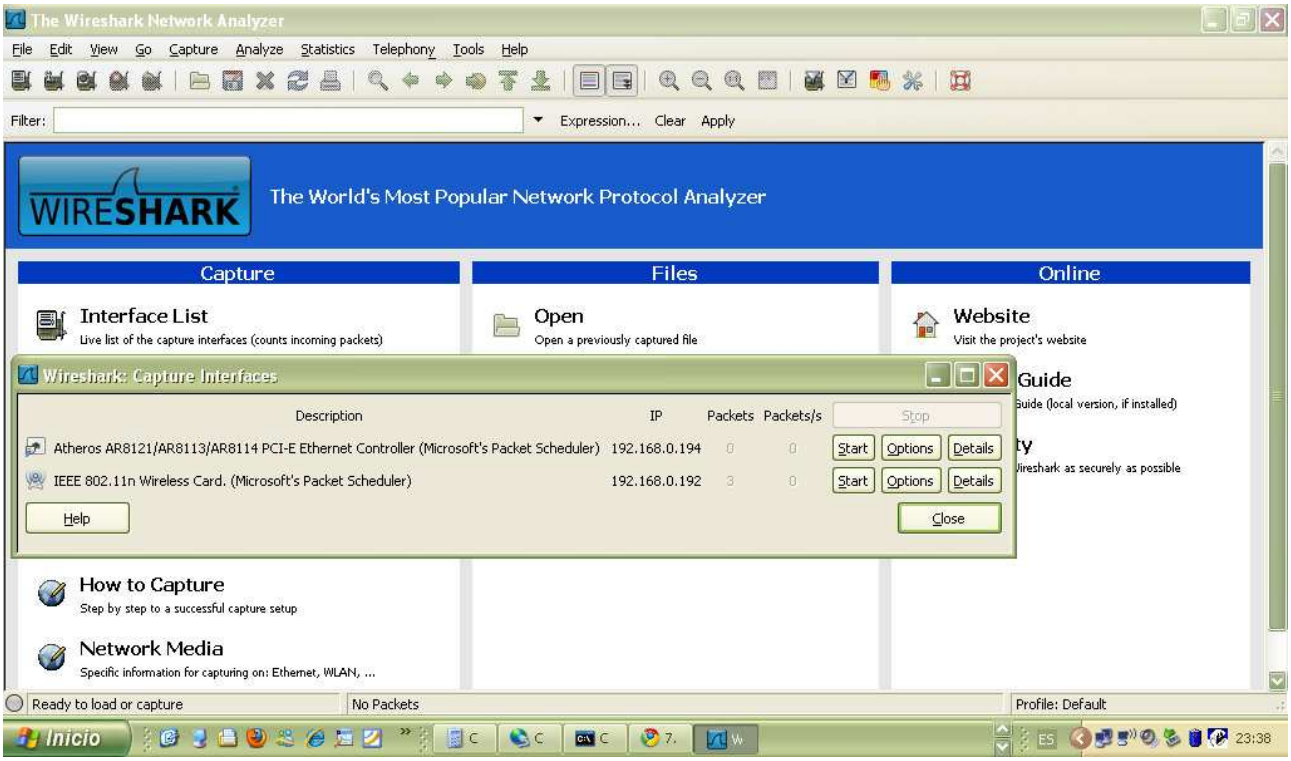


Y al final. Ejecutar el programa:

Vemos las principales opciones:



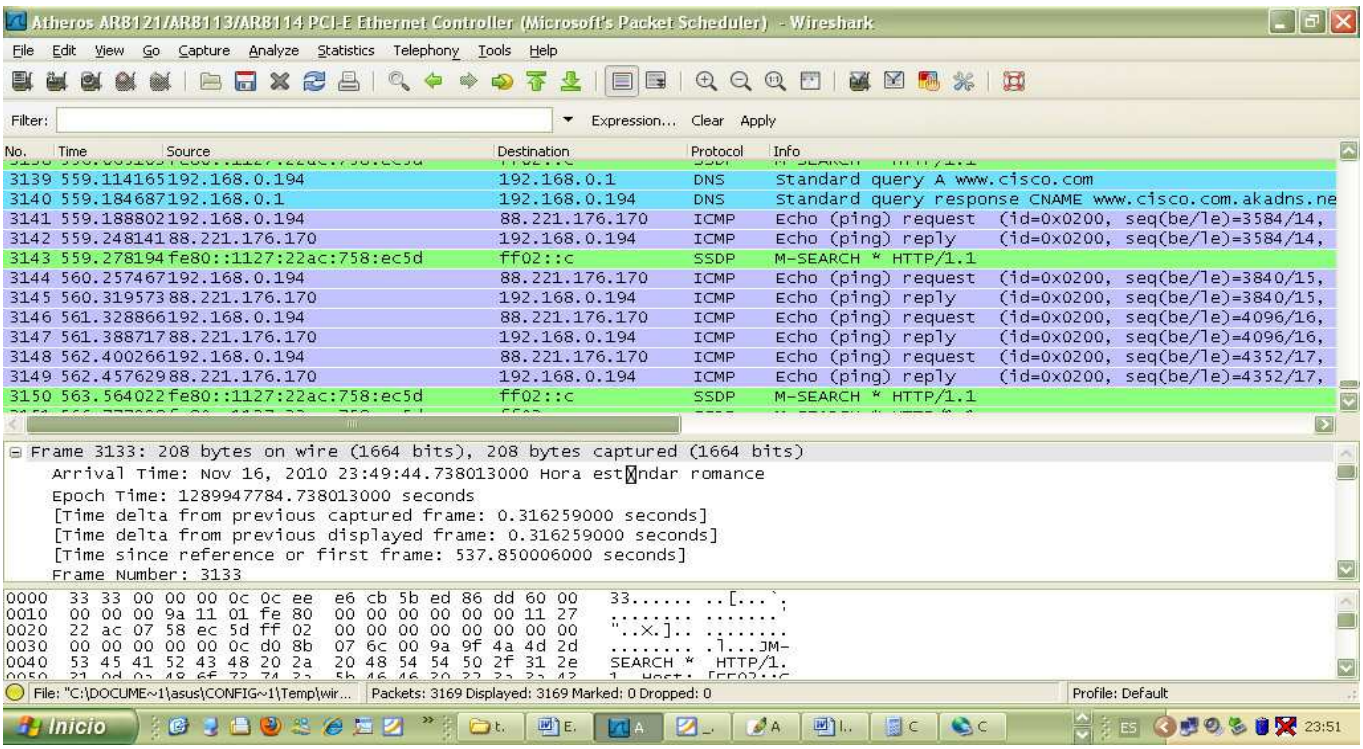
Tras pulsar en Interface list, veremos los adaptadores del PC
En nuestro pc, tenemos dos interfaces: un controlador ethernet y un adaptador wireless



Seleccionamos el adaptador ethernet y pulsamos start para comenzar a capturar paquetes

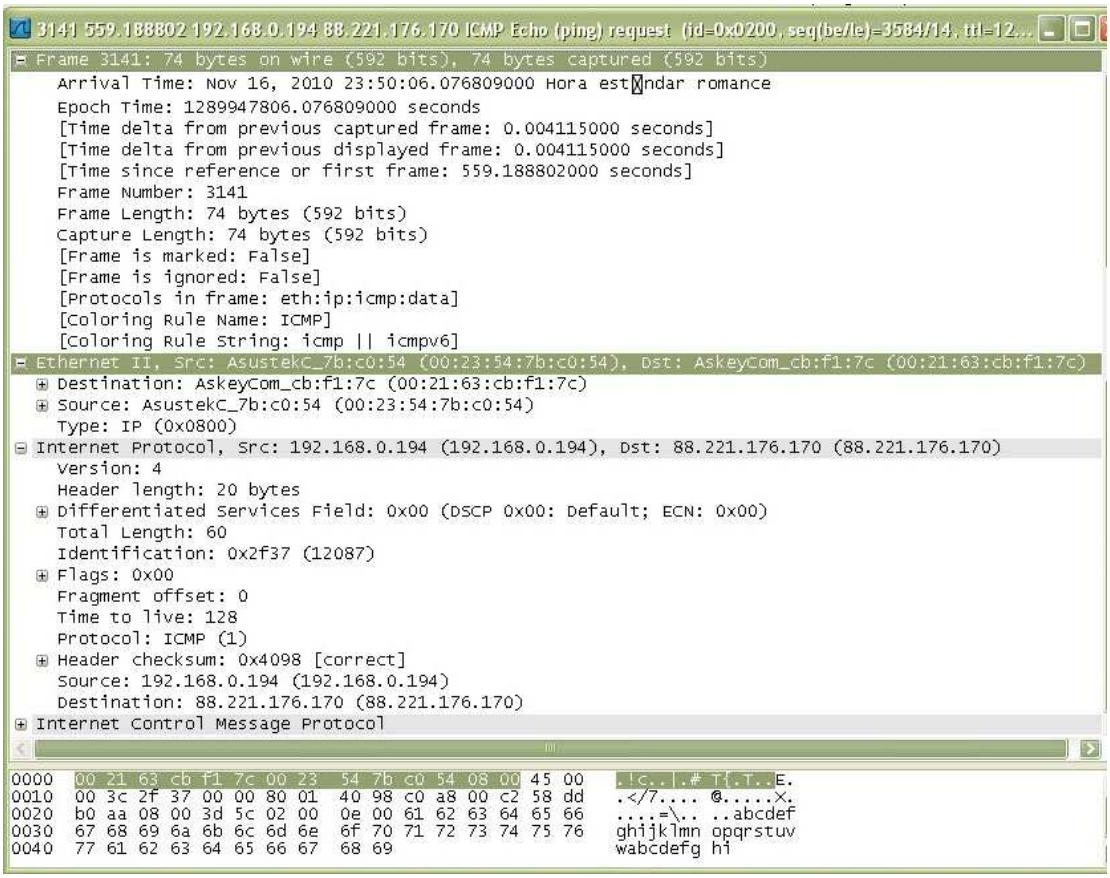
Hacemos un ping a www.cisco.com

Y tras resolver el ping vemos los datos capturados por el wireshark, con los paquetes capturados



Podemos observar que desde la ip del pc (192.168.0.194) pasa por la ip del router (192.168.0.1) para el acceso a internet

Si hacemos doble clic sobre cualquier linea, observaremos al completo la información del paquete, con la información de la trama (ethernet tipo II) y su contenido.



Parte 2: Ejercicio 7.5.2.

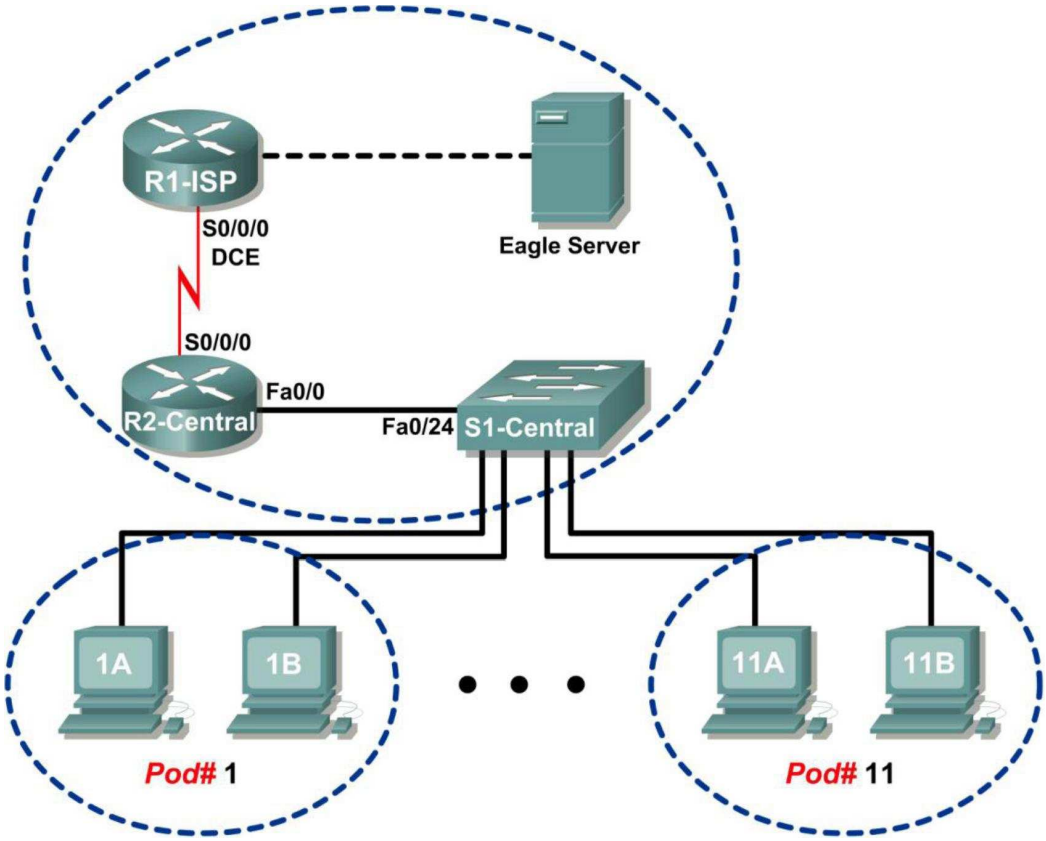


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	No aplicable
	Fa0/0	192.168.254.253	255.255.255.0	No aplicable
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	No aplicable
	Fa0/0	172.16.255.254	255.255.0.0	No aplicable
Eagle Server	No aplicable	192.168.254.254	255.255.255.0	192.168.254.253
	No aplicable	172.31.24.254	255.255.255.0	No aplicable
host*Pod#***A**	No aplicable	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	No aplicable	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	No aplicable	172.16.254.1	255.255.0.0	172.16.255.254

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, usted podrá:

- Explicar los campos de encabezado en una trama de Ethernet II.
- Utilizar Wireshark para capturar y analizar tramas de Ethernet II.

Información básica

Cuando los protocolos de capa superior se comunican entre sí, los datos fluyen hacia abajo en las capas OSI y se encapsulan en la trama de la Capa 2. La composición de la trama depende del tipo de acceso al medio. Por ejemplo, si el protocolo de capa superior es TCP/IP y el acceso al medio es Ethernet, la encapsulación de la trama de la Capa 2 será Ethernet II.

Cuando se aprende sobre los conceptos de la Capa 2, es útil analizar la información del encabezado de la trama. El encabezado de la trama de Ethernet II se examinará en esta práctica de laboratorio. Las tramas de Ethernet II pueden admitir diversos protocolos de la capa superior, como TCP/IP.

Escenario

Se utiliza Wireshark para capturar y analizar los campos de encabezado de tramas de Ethernet II. Si no se cargó Wireshark en la computadora host del módulo, lo puede descargar desde el URL `ftp://eagle-server.example.com/pub/eagle labs/eagle1/chapter7/,` archivo `wireshark-setup-0.99.4.exe.`

El comando **`ping`** de Windows se usa para generar el tráfico de red para que Wireshark capture.

Tarea 1: Explicación de los campos de encabezado en una trama de Ethernet II.

El formato de una trama de Ethernet II se muestra en la Figura 1.

Formato de trama Ethernet II

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 octetos	6 octetos	6 octetos	2 octetos	46- 1500 octetos	4 octetos

Figura 1. Formato de la trama de Ethernet II

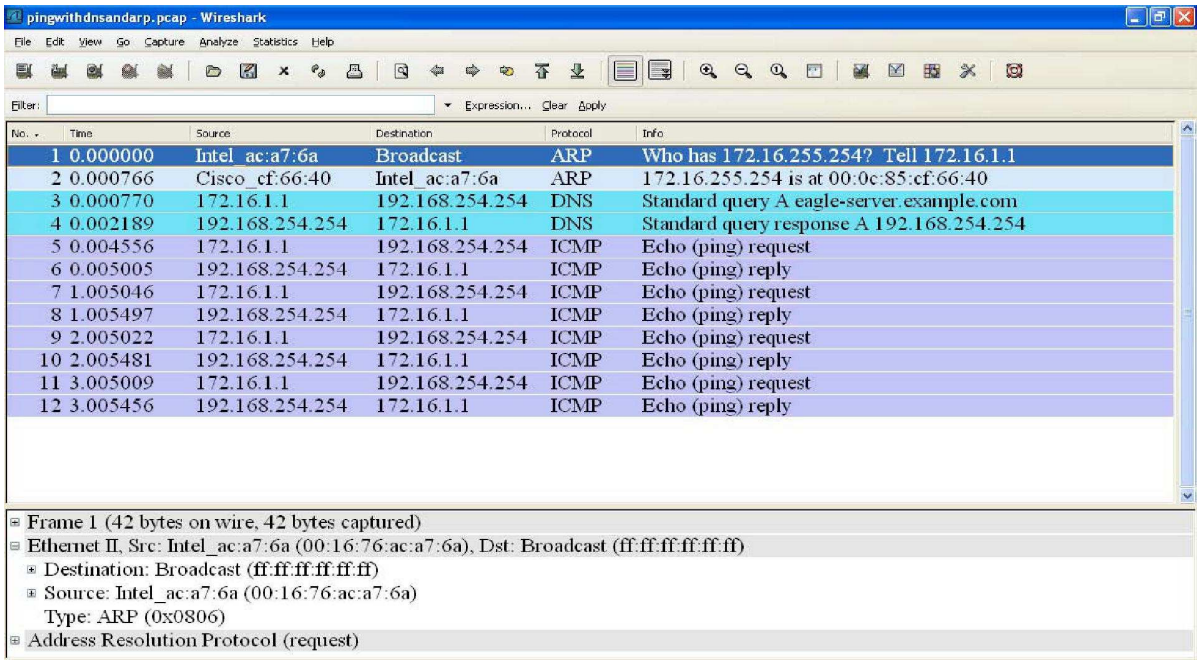


Figura 2. Captura de Wireshark del comando `ping`

En la Figura 2, la ventana de la Lista de panel muestra una captura de Wireshark del comando **`ping`** entre una computadora host del módulo y Eagle Server. La sesión comienza con el protocolo ARP haciendo consultas para la dirección MAC del router de Gateway, seguida de una consulta DNS. Finalmente, el comando **`ping`** emite solicitudes de eco.

En la Figura 2, la ventana de Detalles del paquete muestra la información detallada de la Trama 1. Se puede obtener la siguiente información de la trama de Ethernet II utilizando esta ventana:

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el
Dirección de destino	`ff:ff:ff:ff:ff:ff`	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o 6 bytes, expresado como 12 dígitos hexadecimales, `0-9, A-F`. Un formato común es `12:34:56:78:9A:BC`. Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC). Remítase a http://www.neotechcc.org/forum/macid.htm para obtener una lista de códigos del fabricante. Los últimos seis dígitos hexadecimales, `ac:a7:6a`, representan el número de serie de NIC. La dirección de destino puede ser un broadcast que contiene sólo `1` o unicast. La dirección de origen
Dirección de origen	`00:16:76:ac:a7:6a`	
Tipo de trama	`0x0806`	Para las tramas de Ethernet II, estos campos contienen un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior en el campo de datos. Existen muchos protocolos de capa superior admitidos por

Campo	Valor	Descripción
		comunes de trama son: Valor Descripción `0x0800` Protocolo IPv4 `0x0806` Address resolution protocol (ARP)
Datos	ARP	Contiene el protocolo del nivel superior encapsulado. El campo de datos está entre 46 y 1500 bytes.
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El valor lo computa la máquina de envío, abarcando las direcciones de trama, campos de datos y tipo. El receptor lo verifica.

¿Cuál es el significado de sólo **1** en el campo de dirección de destino?

Que la dirección de destino es la de Broadcast

Conteste las siguientes preguntas sobre la dirección MAC de origen y de destino, con la información que contiene la ventana de Lista de paquetes para la **primera** trama.

Dirección de destino:

Dirección MAC: f f: f f: f f: f f: f f: f f

Fabricante de NIC: No hay

Número de serie de NIC: No hay

Dirección de origen:

Dirección MAC: 00:16:76:ac:a7:6a

Fabricante de NIC: intel

Número de serie de NIC: ac:a7:6a

Conteste las siguientes preguntas sobre la dirección MAC de origen y de destino, con la información que contiene la ventana de Lista de paquetes para la **segunda** trama.

Dirección de destino:

Dirección MAC: 00:16:76:ac:a7:6a

Fabricante de NIC: intel

Número de serie de NIC: ac:a7:6a

Dirección de origen:

Dirección MAC: 00:0c:85:cf:66:40

Fabricante de NIC: cisco

Número de serie de NIC: cf:66:40

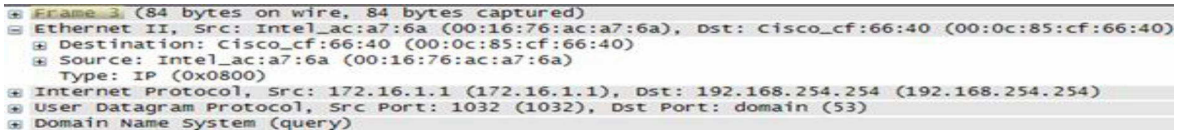


Figura 3. Campos de Trama 3

La figura 3 contiene una vista ampliada de la captura de Wireshark de Trama 3. Utilice la información para completar la siguiente tabla:

Campo	Valor	
Preámbulo	No aparece	
Dirección de	00:0c:85:cf:66:40	192.168.254.254
Dirección de origen	00:16:76:ac:a7:6a	172.16.1.1
Tipo de trama	0x0800	
Datos	IP	
FCS	No aparece	

En la siguiente tarea, Wireshark se utilizará para capturar y analizar paquetes capturados en la computadora host del módulo.

Tarea 2: Utilización de Wireshark para capturar y analizar tramas de Ethernet II.

Paso 1: Configurar Wireshark para las capturas de paquetes.

Prepare Wireshark para las capturas. Haga clic en **Captura > Interfaz**, y luego haga clic en el botón de inicio que corresponde a la dirección IP de interfaz 172.16.x.y. Con esta acción se inicia la captura de paquetes.

Paso 2: Comenzar a hacer ping a Eagle Server y capturar la sesión.

Abra una ventana terminal de Windows. Haga clic en **Inicio > Ejecutar**, escriba **cmd** y haga clic en **Aceptar**.

```
Microsoft Windows XP [Versión
5.1.2600] (C) Copyright 1985-2001
Microsoft Corp.
C:\> ping eagle-
server.example.com
     Pinging eagle-server.example.com      with 32 bytes of
           [192.168.254.254]               data:
Reply from 192.168.254.254:     time<lm TTL=6
bytes=32 Reply from             s       2
192.168.254.254: bytes=32 Reply time<lm TTL=6
from 192.168.254.254: bytes=32  s       2
Reply from 192.168.254.254:     time<lm TTL=6
Ping statistics for 192.168.254.254:      loss),
   Packets: Sent = 4, Received = 4, Lost
= 0 (0% Approximate round trip times in
milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average =
C:\>
```

Figura 4. Ping a eagle-server.example.com

Haga ping a eagle-server.example.com como se muestra en la Figura 4. Cuando el comando haya finalizado la ejecución, detenga las capturas de Wireshark.

Paso 3: Analizar la captura de Wireshark.

La ventana de la Lista de paquetes de Wireshark debe comenzar con una solicitud y respuesta ARP para la dirección MAC del Gateway. Luego, se realiza una solicitud DNS para la dirección IP de eagle-server.example.com. Finalmente, se ejecuta el comando **`ping`**. La captura debe verse similar a la que se mostró en la Figura 2.

El siguiente paso, lo realizo dos veces:
con los datos que obtengo de la practica 7.5.2, metiendo los datos en el packet trace,
y posteriormente con un ping a www.cisco.com desde mi ordenador

CON LOS DATOS DEL PACKET TRACE:

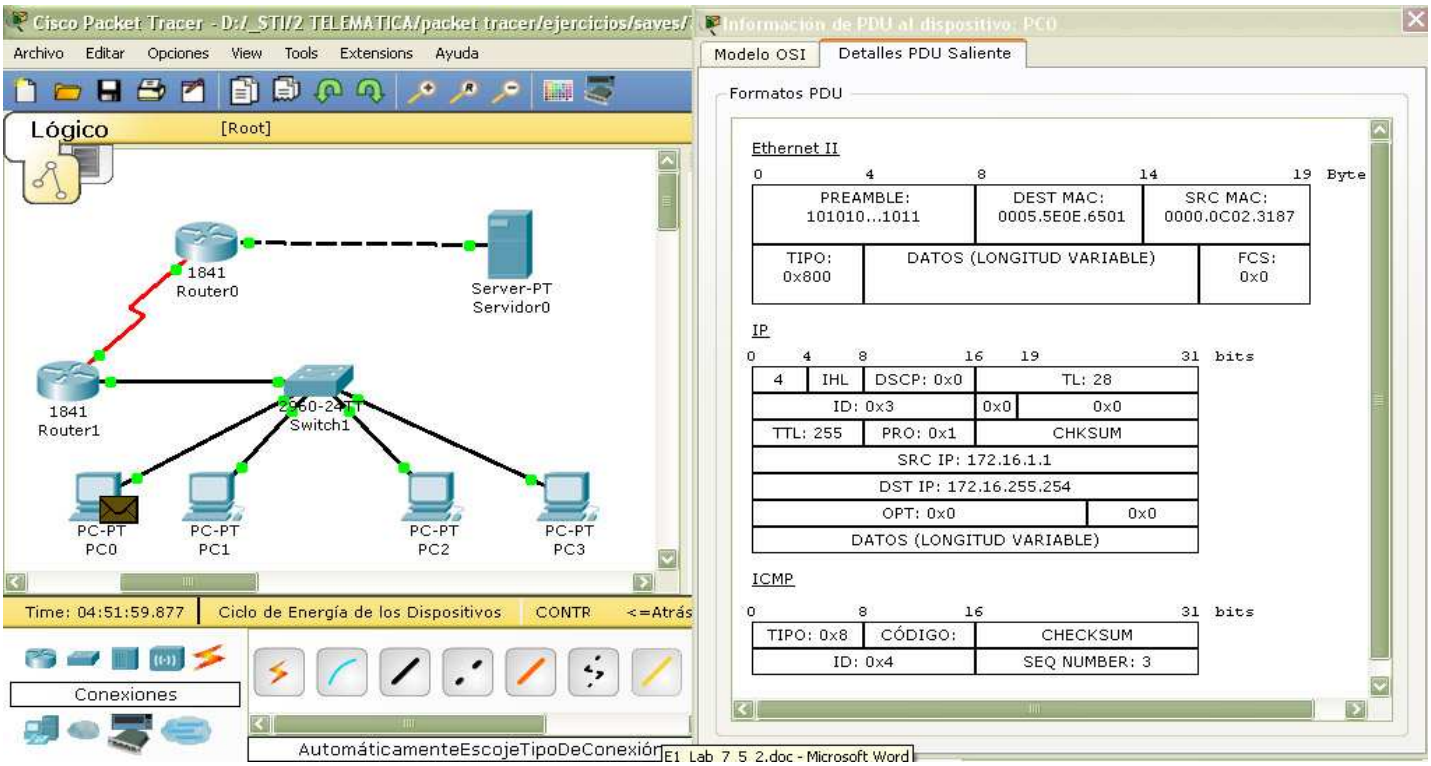
Utilice la captura de Wireshark del comando **`ping`** para contestar las siguientes preguntas:

Información de la dirección MAC de la computadora del módulo. :en este caso tomo PC0

Dirección MAC: 00:00:0c:02:31:87
Fabricante de NIC: Cisco
Número de serie de NIC: 02:31:87

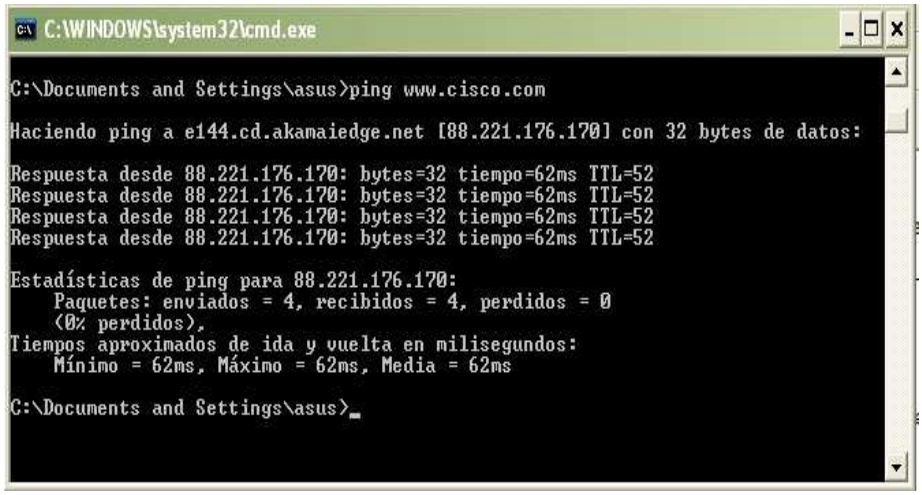
Información de la dirección MAC de R2-Central:

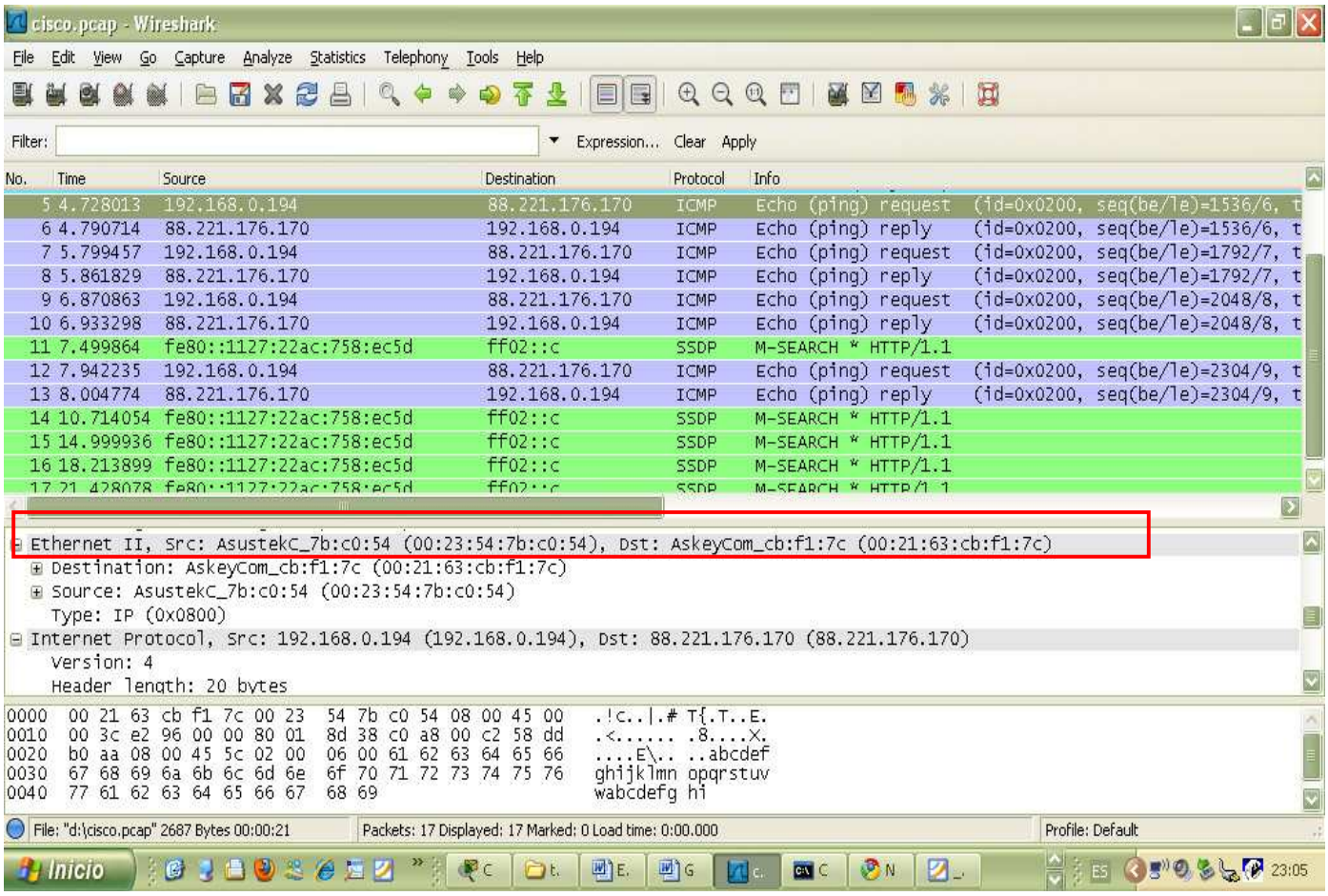
Dirección MAC: 00:05:5e:0e:65:01
Fabricante de NIC: Cisco Systems
Número de serie de NIC: 0e:65:01



CON EL DATO www.cisco.com en WIRESHARK conectados a Internet

Primero hacemos un ping a www.cisco.com y observamos wireshark





Utilice la captura de Wireshark del comando **`ping`** para contestar las siguientes preguntas:

Información de la dirección MAC de la computadora del módulo. :origen

Dirección MAC: 00:23:54:7b:c0:54
Fabricante de NIC: asustek computer inc
Número de serie de NIC: 7b:c0:54

Información de la dirección destino:

Dirección MAC: 00:21:63:cb:f1:7c
Fabricante de NIC: askeycom
Número de serie de NIC: cb:f1:7c

Un estudiante de otra escuela quisiera saber la dirección MAC para Eagle Server. ¿Qué le diría al estudiante? No lo puede saber porque no esta en la misma red y las MAC solo se ven en esa LAN.

¿Cuál es el valor del tipo de trama de Ethernet II para una solicitud ARP? 0x806

¿Cuál es el valor del tipo de trama de Ethernet II para una respuesta ARP? 0x806

¿Cuál es el valor del tipo de trama de Ethernet II para una solicitud ARP? 0x806

¿la misma pregunta?

¿Cuál es el valor del tipo de trama de Ethernet II para una respuesta de solicitud DNS? 0x800

¿Cuál es el valor del tipo de trama de Ethernet II para un eco ICMP? 0x800

¿Cuál es el valor del tipo de trama de Ethernet II para una respuesta de eco ICMP? 0x800

Tarea 4: Reflexión

En esta práctica de laboratorio se examinó la información del encabezado de trama de Ethernet II. Un campo de preámbulo contiene siete bytes de secuencias que alternan `0101,` y un byte que indica el inicio de la trama, `01010110.` Cada una de las direcciones MAC de origen y de destino contiene 12 dígitos hexadecimales. Los primeros seis dígitos hexadecimales contienen el fabricante de la NIC y los últimos seis dígitos contienen el número de serie de NIC. Si la trama es broadcast, la dirección MAC de destino contiene sólo 1. Un campo del tipo de trama de 4 bytes contiene un valor que indica el protocolo en el campo de datos. El valor para IPv4 es `0x0800.` El campo de datos es variable y contiene el protocolo de capa superior encapsulado. Al final de la trama, se utiliza el valor FCS de 4 bytes para verificar que no hubo errores durante la transmisión.

Tarea 5: Limpieza

Se instaló Wireshark en la computadora host del módulo. Si debe desinstalarlo, haga clic en **Inicio > Panel de control**. Abra **Agregar o quitar programas**. Marque Wireshark y haga clic en **Quitar**.

Elimine todos los archivos creados durante la práctica de laboratorio en la computadora host del módulo.

A menos que el instructor le indique lo contrario, apague las computadoras host. Llévese todo aquello que haya traído al laboratorio y deje el aula lista para la próxima clase.