

**SISTEMAS INFORMÁTICOS - TEMA9**  
**Práctica: Introducción a las redes****CFGS**  
**DAM****ÍNDICE**

<u>Introducción.....</u>	<u>2</u>
<u>Objetivos de la práctica.....</u>	<u>2</u>
<u>Cables UTP.....</u>	<u>2</u>
<u>Protocolos.....</u>	<u>3</u>
<u>Protocolo ARP.....</u>	<u>3</u>
<u>Wiresark.....</u>	<u>5</u>

**SISTEMAS INFORMÁTICOS - TEMA9**  
**Práctica: Introducción a las redes****CFGS**  
**DAM****Introducción**

La documentación a entregar será **un archivo pdf** con la información que se pide y que se encuentra en negrita. **No copies toda la práctica por favor.**

# **Objetivos de la práctica**

Los objetivos que se buscan con esta práctica son:

- Que el alumno busque información sobre algunos componentes de las redes
- Que el alumno investigue algunos de los puertos más utilizados en las redes

**Cables UTP**

**Completa la siguiente tabla en tu documento**

	Velocidad máxima	Frecuencia	Distancia máxima	Observaciones
Categoría 5	100 Mbps	100 Mhz	100 m	Actualmente obsoleto. Use RJ-45
Categoría 5e	1Gbps	100MHz	100m	
Categoría 6	1Gbps	250MHz	100m	
Categoría 6En	10Hbps	500MHz	100m	
Categoría 7	10Gbps	600MHz	100m	
Categoría 7En	10Gbps	1000MHz	100m	
Categoría 8	40Gbps	2000MHz	30m	
Categorías 9 y 10	10Gbps		100m	
Cable coaxial	10Gbps	2.150MHz	2.4KM	

## SISTEMAS INFORMÁTICOS - TEMA9

### Práctica: Introducción a las redes

**CFGS  
DAM**

## Protocolos

Averigua cuáles son los puertos de los siguientes protocolos utilizados de la capa de aplicación:  
**Completa la siguiente tabla en tu documento**

	Puerto	Utilidad (breve descripción del protocolo)
DNS	53	Resolucion de nombres de dominio
DHCP	67 - 68	Configuracion de red automatica
SMTP	25 – 465 – 587 - 2525	Transferencia simple de correo
POP	110	Transferencia de correo
FTP	20 - 21	Transferencia de archivos
TELNET	23	Conexion de equipos remota
SSH	22	Administracion remota de equipos
HTTP	80	Transferencia de hipertexto
LDAP	389	Acceso a directorios remotos
PING	No es un protocolo. El protocolo que usa el ping es el icmp, aunque este no tiene concepto de puertos	Prueba de conexión con otro equipo

*Tabla 1. Protocolos*

## Protocolo ARP

Busca información sobre el protocolo ARP.

**Protocolo ARP:**

**SISTEMAS INFORMÁTICOS - TEMA9**  
**Práctica: Introducción a las redes****CFGS**  
**DAM**

Una vez tenemos claro que es el protocolo ARP debes conseguir los siguientes datos de dos NIC, la de tu ordenador y la de tu router (puerta de enlace predeterminada)

Abajo tienes una tabla, rellénala con tu IP. Para obtener la IP puedes hacer un «ipaddr/ifconfig» y ver la de tu router fijado en la "puerta de enlace predeterminada". Éste es tu router, **es tu puerta de salida al exterior**.

Adaptador de LAN inalámbrica Wi-Fi 2:

```
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::c4c0:e116:bb46:7a68%18  
Dirección IPv4. . . . . : 192.168.0.19  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 192.168.0.1
```

**router**

Investiga cómo obtendrías la dirección MAC de tu ordenador.

Para obtener la dirección IP del router que te da la salida a Internet puede realizar, en Linux, la siguiente orden:

```
route -r
```

En la primera entrada tienes tu puerta de enlace predeterminada

```
administrador@eduardoSapinyaExamenSI:~$ route -n  
Tabla de rutas IP del núcleo  
Destino      Pasarela      Genmask      Indic Métric Ref      Uso Interfaz  
0.0.0.0      10.0.2.2      0.0.0.0      UG    100    0        0 enp0s3  
10.0.2.0     0.0.0.0      255.255.255.0 U    100    0        0 enp0s3  
169.254.0.0  0.0.0.0      255.255.0.0  U    1000   0        0 enp0s3
```

Para obtener la MAC del router puedes consultar la tabla ARP que es dinámica (desaparece cuando apagamos el ordenador y se construye cuando lo arrancamos). Para conocer de qué estamos hablando haz el siguiente comando en tu Linux o Windows:

```
arp -a
```

1. Datos que necesitamos conocer antes de empezar:
  - La dirección IP de tu ordenador y dirección física de la interfaz de red (NIC)  
172.31.22.38/26 08:00:27:f3:91:e9
  - La dirección IP de tu compañero (no le pides la MAC)
  - Tu máquina virtual debe estar configurada en modo «*adaptador puente*»
2. Instalación de Wireshark

## SISTEMAS INFORMÁTICOS - TEMA9

### Práctica: Introducción a las redes

**CFGS  
DAM**

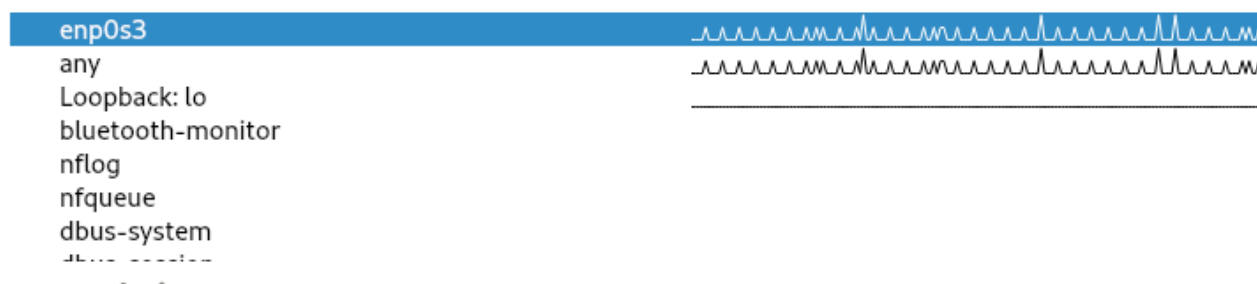
- <https://howtoforge.es/como-instalar-el-analizador-de-paquetes-de-red-wireshark-en-ubuntu-20-04/>
- Si no puedes instalarlo desde este enlace busca otro.

3. Abre Wireshark. Es posible que veas protocolos que te suenen o que hayamos visto.
4. Para que sea más fácil la lectura de datos aplicaremos un filtro para mostrar las PDU de ICMP (protocolo utilizado para realizar un ping). Escribe icmp en el cuadro Filter

Welcome to Wireshark

### Capturar


...usando este filtro:



## CAPTURA Y ANÁLISIS DE DATOS ICMP LOCALES

5. Ahora han desaparecido todos los datos pero sigue capturando información. Vamos a capturar el tráfico del protocolo ICMP. Abre un terminal y haz un ping a tu compañero (recuerda que ping utiliza el protocolo ICMP). Cuando tengas un par de paquetes para el ping, si estás en Linux.

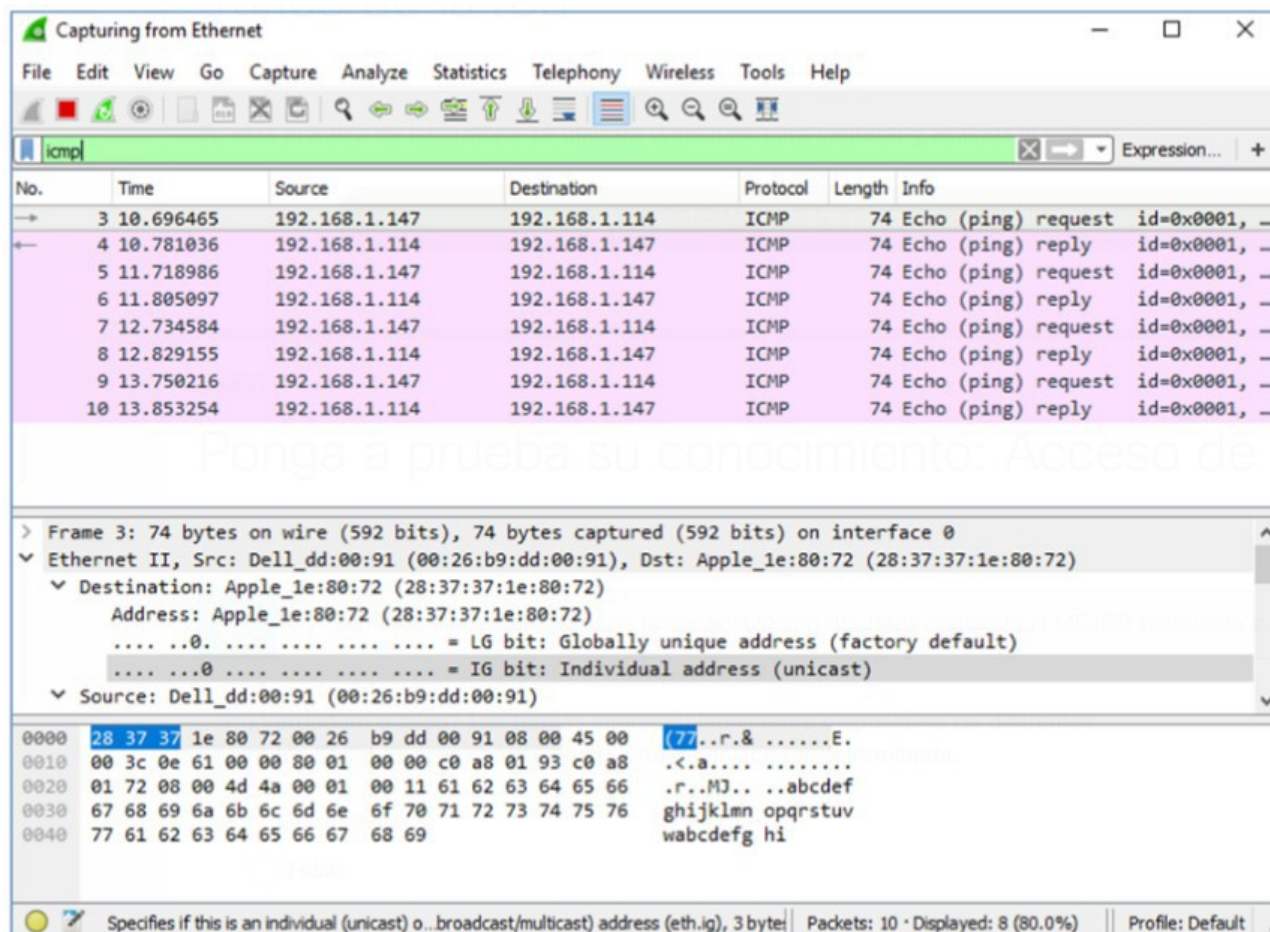
No.	Time	Source	Destination	Protocol	Length	Info
3	2.051365341	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)
4	2.075359665	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)
5	4.099023611	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)
6	5.123959154	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)
7	6.148122907	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)
8	7.178739737	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)
9	8.195162120	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)
10	9.219295532	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)
11	10.243182589	172.30.22.38	170.30.22.42	ICMP	98	Echo (ping)

6. La ventana del Wireshark es como ésta. Cuando capturas un buen puñado de paquetes puede pararlo  pulsando en

## SISTEMAS INFORMÁTICOS - TEMA9

### Práctica: Introducción a las redes

**CFGS  
DAM**



7. Los datos de Wireshark se muestran en tres secciones:
  - a) La sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada,
  - b) La sección intermedia muestra información de la PDU para la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas de protocolo, y
  - c) La sección inferior muestra los datos sin procesar de cada capa. Los datos sin procesar se muestran en formatos hexadecimal y decimal
- Haz clic en alguna de las primeras tramas de PDU de la solicitud de ICMP en la sección superior de Wireshark. Observa que la columna Source contiene la dirección IP de tu PC y la columna Destination contiene la dirección IP del PC de tu compañero al que hiciste ping.
- Con esta trama de PDU todavía seleccionada en la sección superior, fijado en la sección intermedia. Haz clic en el signo más que está a la izquierda de la fila de Ethernet II para ver las direcciones MAC de origen y destino.

### 8. Contesta a las siguientes preguntas

- a) ¿La dirección MAC de origen coincide con la MAC de tu PC?

SI



**SISTEMAS INFORMÁTICOS - TEMA9**  
**Práctica: Introducción a las redes****CFGS  
DAM**

- b) ¿Cómo obtiene tu PC la dirección MAC del PC al que le hizo ping?  
Mediante el protocolo ARP

## **CAPTURA Y ANÁLISIS DE DATOS HTTP REMOTOS**

9. En esta segunda parte generaremos datos HTTP visitando algunas páginas web y compararemos los datos obtenidos con los de la parte anterior
- Abre el navegador de tu equipo y vuelve a iniciar la captura de datos
  - Si te pregunta si quieres guardar los datos capturados anteriormente dile que NO
  - En tu navegador visita la web [www.cisco.com](http://www.cisco.com)
  - Cuando cargue la página web y haya capturado datos en la comunicación ya podrás responder a las siguientes preguntas.
10. Selecciona una línea del protocolo HTTP. ¿Cuáles son ahora las direcciones IP y MAC de destino? **Alguna se parece a las obtenidas anteriormente?**

```
▶ Frame 10: 175 bytes on wire (1400 bits), 175 bytes captured
▼ Ethernet II, Src: Guangzho_5b:5c:84 (f4:20:15:5b:5c:84), Dst
  ▶ Destination: IPv4mcast_7f:ff:96 (01:00:5e:7f:ff:96)
  ▶ Source: Guangzho_5b:5c:84 (f4:20:15:5b:5c:84)
    Type: IPv4 (0x0800)
  ▶ Internet Protocol Version 4, Src: 172.30.22.44, Dst: 239.255
  ▶ User Datagram Protocol, Src Port: 2990, Dst Port: 2990
  ▶ Data (133 bytes)
```

**No se parecen**

11. Reflexiona, ¿por qué WireShark muestra la dirección MAC de los hosts locales, pero no la dirección MAC de los hosts remotos?  
porque los paquetes enviados y recibidos dentro de la red local contienen la dirección MAC de origen y destino. Sin embargo, para los hosts remotos, las direcciones MAC no se transmiten directamente dentro de los paquetes.