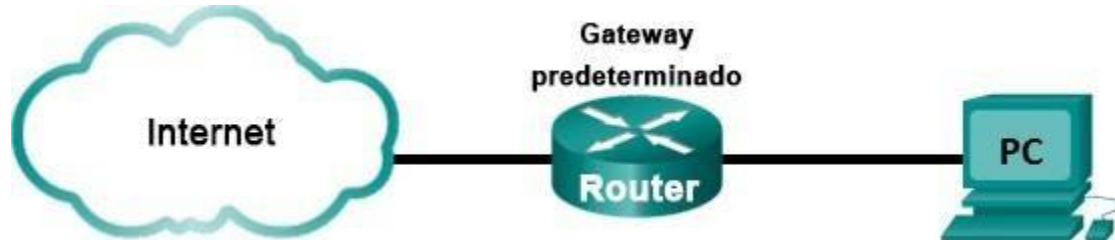


## Práctica de laboratorio: Uso de Wireshark para examinar tramas de Ethernet.

### Topología



### Objetivos

**Parte 1:** Examinar los **campos de encabezado** en una trama de Ethernet

#### Información básica/Situación

Cuando los protocolos de la capa superior se comunican entre sí, los datos fluyen hacia abajo en las capas de interconexión 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 los protocolos de capa superior son TCP e IP, y el acceso al medio es Ethernet, la encapsulación de la trama de la capa 2 será Ethernet.

Esto es típico de un entorno LAN.

Cuando se aprende sobre los conceptos de la capa 2, es **útil analizar la información del encabezado de la trama.**

## Parte 1: Examinar los campos de encabezado en una trama de Ethernet

**Paso 1:** Revisar las **descripciones y las longitudes de los campos de encabezado de Ethernet**

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

**Dirección MAC: XX:XX:XX:XX:XX:XX Cada X son 4 bits**

**Paso 2:** Examinar la configuración de red del PC

```
Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . : cisco.com
    Vínculo: dirección IPv6 local. . . . . : fe80::b875:731b:3c7b:c0b1
    Dirección IPv4. . . . . : 10.20.164.22
    Máscara de subred . . . . . : 255.255.255.240
    Puerta de enlace predeterminada . . . . : 10.20.164.17
```

- **1¿La dirección IP del host de tú PC es? ¿Y tú MAC?**

```
C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : 
    Vínculo: dirección IPv6 local. . . : fe80::f5e2:42d3:df75:6bc9%11
    Dirección IPv4. . . : 192.168.12.16
    Máscara de subred. . . : 255.255.255.0
    Puerta de enlace predeterminada. . . : 192.168.12.1

Adaptador de túnel isatap.{C8BA642E-5586-4D4E-B32F-F39510A1D16F}:

    Estado de los medios. . . : medios desconectados
    Sufijo DNS específico para la conexión. . : 

C:\Windows\system32>ipconfig /all

Configuración IP de Windows

    Nombre de host. . . : 16B12
    Sufijo DNS principal. . . : 
    Tipo de nodo. . . : híbrido
    Enrutamiento IP habilitado. . . : no
    Proxy WINS habilitado. . . : no

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . : 
    Descripción. . . : Realtek PCIe GBE Family Controller
    Dirección física. . . : 2C-4D-54-D4-FB-AB
    DHCP habilitado. . . : no
    Configuración automática habilitada. . . : sí
    Vínculo: dirección IPv6 local. . . : fe80::f5e2:42d3:df75:6bc9%11(Preferido)

    Dirección IPv4. . . : 192.168.12.16(Preferido)
    Máscara de subred. . . : 255.255.255.0
    Puerta de enlace predeterminada. . . : 192.168.12.1
    IAID DHCPv6. . . : 241190347
    DUID de cliente DHCPv6. . . : 00-01-00-01-23-3D-53-B8-2C-4D-54-D4-FB-AB
    Servidores DNS. . . : 192.168.12.1
    NetBIOS sobre TCP/IP. . . : habilitado
```

- **2¿La dirección IP del gateway predeterminado es? ¿Y la MAC?**

```
C:\Windows\system32>arp -a

Interfaz: 192.168.12.16 --- 0xb
    Dirección de Internet      Dirección física      Tipo
    192.168.12.1              6c-3b-6b-32-44-f8    dinámico
```

### Paso 3: Examinar las **tramas de Ethernet** en una **captura de Wireshark**

En la siguiente captura de Wireshark, se muestran los paquetes que generó un ping que se emitió desde un host del PC hasta su gateway predeterminado.

#### **ping dirección\_IP\_gateway**

Se aplicó un **filtro a Wireshark para ver los protocolos ARP e ICMP únicamente**. La sesión comienza con una **consulta de ARP** para la dirección MAC del router del gateway, seguida de **cuatro solicitudes y respuestas de ping**.

- **3“Muestra una captura de pantalla”**

*Realtek PCIe GBE Family Controller: Conexión de área local						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
arp or icmp						
No.	Time	Source	Destination	Protocol	Length	Info
448	26.439716	192.168.12.16	23.37.160.19	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=64 (reply in 449)
449	26.458749	23.37.160.19	192.168.12.16	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=55 (request in 448)
450	26.546384	HewlettP_fc:59:37	Broadcast	ARP	60	Who has 192.168.12.100? Tell 192.168.12.4
455	26.593618	AsustekC_65:c5:54	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.78
456	26.597488	AsustekC_6a:d9:54	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.19
471	27.435235	192.168.12.16	23.37.160.19	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=64 (reply in 473)
472	27.439928	AsustekC_6a:ca:5a	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.70
473	27.455119	23.37.160.19	192.168.12.16	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=55 (request in 471)
514	27.884953	Giga-Byt_9f:ab:1b	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.26
515	27.888190	AsustekC_d4:fd:10	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.20
516	28.033950	AsustekC_6a:bc:b6	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.33
530	28.267526	HewlettP_fc:59:37	Broadcast	ARP	60	Who has 192.168.12.11? Tell 192.168.12.4
531	28.349664	AsustekC_d4:f4:bb	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.89
540	28.433600	192.168.12.16	23.37.160.19	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=64 (reply in 541)
541	28.451328	23.37.160.19	192.168.12.16	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=55 (request in 540)
542	28.655505	AsustekC_d4:fb:ab	Broadcast	ARP	42	Who has 192.168.12.4? Tell 192.168.12.16
543	28.656341	HewlettP_fc:59:37	AsustekC_d4:fb:ab	ARP	60	192.168.12.4 is at fc:15:b4:fc:59:37
553	28.694787	HewlettP_fc:59:37	Broadcast	ARP	60	Who has 192.168.12.17? Tell 192.168.12.4
554	28.711595	AsustekC_6a:d9:5a	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.112
555	28.712961	AsustekC_d4:fb:8d	Broadcast	ARP	60	Who has 192.168.12.4? Tell 192.168.12.22
594	29.447508	192.168.12.16	23.37.160.19	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=64 (reply in 595)
595	29.461589	23.37.160.19	192.168.12.16	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=55 (request in 594)

▶ Frame 594: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 ▶ Ethernet II, Src: AsustekC_d4:fb:ab (2c:4d:54:d4:fb:ab), Dst: Routerbo_32:44:f8 (6c:3b:6b:32:44:f8) ▶ Destination: Routerbo_32:44:f8 (6c:3b:6b:32:44:f8) Address: Routerbo_32:44:f8 (6c:3b:6b:32:44:f8) ....0. .... = LG bit: Globally unique address (factory default) ....0. .... = IG bit: Individual address (unicast) ▶ Source: AsustekC_d4:fb:ab (2c:4d:54:d4:fb:ab) Address: AsustekC_d4:fb:ab (2c:4d:54:d4:fb:ab) ....0. .... = LG bit: Globally unique address (factory default) ....0. .... = IG bit: Individual address (unicast) Type: IPv4 (0x0800) ▶ Internet Protocol Version 4, Src: 192.168.12.16, Dst: 23.37.160.19 ▶ Internet Control Message Protocol
---

**Paso 4:** Examinar el **contenido de encabezado** de Ethernet de una solicitud de ARP En la tabla siguiente, se toma la **primera trama** de la captura de Wireshark y se muestran los **datos de los campos de encabezado** de Ethernet.

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de NIC.
Dirección de destino	Broadcast (ff:ff:ff:ff:ff:ff)	Direcciones de la Capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o seis octetos, expresada como 12 dígitos hexadecimales, 0-9, A-F.
Dirección de origen	Dell_24:2a:60 (5c:26:0a:24:2a:60)	Un formato común es 12:34:56:78:9A:BC. Los <b>primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC)</b> ; los <b>seis últimos números hexadecimales corresponden al número de serie de la NIC</b> . La dirección de destino puede ser un broadcast, que contiene todos unos, o un unicast. La dirección de origen es siempre unicast.
Tipo de trama	0x0806	Para las tramas de Ethernet II, estos campos contienen un valor hexadecimal que se utiliza para <b>indicar el tipo de protocolo de capa superior en el campo de datos</b> . Existen muchos protocolos de capa superior que admite Ethernet II. Dos tipos comunes de trama son: <div> <div>Valor</div> <div>Descripción</div> </div> 0x0800 Protocolo IPv4 0x0806 Protocolo de resolución de direcciones (ARP)
Datos	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos está entre 46 y 1,500 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.

- **4 Muestra una captura de pantalla y marca los datos de cada uno de los campos de una trama estudiados más arriba.**

## ARP

Wireshark capture of an ARP request packet. The packet list shows three frames, with the third frame (No. 584) selected. The packet details pane shows the Ethernet II header, ARP (Type: ARP) padding, and the Address Resolution Protocol (request) section. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
310	6.642430	Giga-Byt_9f:ab:1b	Broadcast	ARP	60	Who has 192.168.12.78? Tell 192.168.12.26
558	7.323782	AsustekC_6a:bc:b6	Broadcast	ARP	60	Who has 192.168.12.78? Tell 192.168.12.33
584	8.088831	AsustekC_d4:fd:10	Broadcast	ARP	60	Who has 192.168.12.78? Tell 192.168.12.20

Frame 310: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

- Interface id: 0 (\Device\NPF\_{C8BA642E-5586-4D4E-B32F-F39510A1D16F})
- Interface name: \Device\NPF\_{C8BA642E-5586-4D4E-B32F-F39510A1D16F}
- Encapsulation type: Ethernet (1)
- Arrival Time: Feb 14, 2019 15:49:48.896778000 Hora estándar romance
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1550155788.896778000 seconds
- [Time delta from previous captured frame: 0.019778000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 6.642430000 seconds]
- Frame Number: 310
- Frame Length: 60 bytes (480 bits)
- Capture Length: 60 bytes (480 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:arp]
- [Coloring Rule Name: ARP]
- [Coloring Rule String: arp]

Ethernet II, Src: Giga-Byt\_9f:ab:1b (50:e5:49:9f:ab:1b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  - Address: Broadcast (ff:ff:ff:ff:ff:ff)
  - ... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
  - ... ..1. .... = IG bit: Group address (multicast/broadcast)
- Source: Giga-Byt\_9f:ab:1b (50:e5:49:9f:ab:1b)
  - Address: Giga-Byt\_9f:ab:1b (50:e5:49:9f:ab:1b)
  - ... ..0. .... = LG bit: Globally unique address (factory default)
  - ... ..0. .... = IG bit: Individual address (unicast)

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: Giga-Byt\_9f:ab:1b (50:e5:49:9f:ab:1b)

0000 ff ff ff ff ff 50 e5 49 9f ab 1b 08 06 00 01 .....P. I....

0010 08 00 06 04 00 01 50 e5 49 9f ab 1b c0 a8 0c 1a .....P. I.....

0020 00 00 00 00 00 00 c0 a8 0c 4e 00 00 00 00 00 00 .....N.....

## ICMP

\*Realtek PCIe GBE Family Controller: Conexión de área local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
39635	986.286112	192.168.12.16	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 39636)
39636	986.287054	192.168.12.1	192.168.12.16	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 39635)
39673	987.293207	192.168.12.16	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 39674)
39674	987.294067	192.168.12.1	192.168.12.16	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 39673)
39773	988.306889	192.168.12.16	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 39774)
39774	988.307789	192.168.12.1	192.168.12.16	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 39773)
39840	989.320939	192.168.12.16	192.168.12.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 39841)
39841	989.321830	192.168.12.1	192.168.12.16	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 39840)

[Coloring Rule String: icmp || icmpv6]

- Ethernet II, Src: AsustekC\_d4:fb:ab (2c:4d:54:d4:fb:ab), Dst: Routerbo\_32:44:f8 (6c:3b:6b:32:44:f8)
  - Destination: Routerbo\_32:44:f8 (6c:3b:6b:32:44:f8)
    - Address: Routerbo\_32:44:f8 (6c:3b:6b:32:44:f8)
      - ....0.... = LG bit: Globally unique address (factory default)
      - ....0.... = IG bit: Individual address (unicast)
    - Source: AsustekC\_d4:fb:ab (2c:4d:54:d4:fb:ab)
      - Address: AsustekC\_d4:fb:ab (2c:4d:54:d4:fb:ab)
        - ....0.... = LG bit: Globally unique address (factory default)
        - ....0.... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.12.16, Dst: 192.168.12.1

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4d5a [correct]  
[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

[Response frame: 39636]

Data (32 bytes)

```

0000  6c 3b 6b 32 44 f8 2c 4d 54 d4 fb ab 08 00 45 00  l;k2D.,M T...E
0010  00 3c 62 5d 00 00 40 01 00 00 c0 a8 0c 10 c0 a8  <bj..@: .....
0020  0c 01 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66  ....MZ...abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
  
```