UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
FACULTAD DE INGENIERÍA

TALLER 1 ASPECTOS BÁSICOS DE ENLACE DE DATOS
FUNDAMENTOS DE REDES DE COMUNICACIONES

Juan David Orduz Sastoque - 20221020096
Daniel David Cuellar - 20221020081

PROFESOR
PAULO ALONSO GAONA GARCIA

Bogotá D.C.
2025

ASPECTOS BÁSICOS DE ENLACE DE DATOS

INTRODUCCIÓN

En este taller se busca comprender de manera práctica cómo funciona la capa de enlace de datos dentro de una red, observando cómo se transmiten las tramas Ethernet y cómo los dispositivos utilizan las direcciones MAC para comunicarse entre sí. Para ello se emplean herramientas como Wireshark, que permite capturar y analizar el tráfico de red, y switches Cisco (en Cisco Packet Tracer), que facilitan la visualización de las tablas de direcciones MAC. De esta forma, el ejercicio refuerza los conceptos teóricos vistos en clase y acerca al estudiante a la experiencia real de diagnosticar y entender el comportamiento de una red local.

OBJETIVOS

Objetivo General

Comprender y aplicar los conceptos fundamentales del enlace de datos mediante el análisis de tramas Ethernet y la observación de tablas MAC, utilizando herramientas de monitoreo y equipos de red para fortalecer las competencias en el diagnóstico y administración de redes de comunicaciones.

Objetivos específicos

- Examinar los campos de encabezado de una trama de Ethernet II
- Utilizar Wireshark para capturar y analizar tramas de Ethernet
- Armar y configurar la red
- Examinar la tabla de direcciones MAC del switch

DESARROLLO

PARTE 1

A continuación se examinarán los campos de encabezado y el contenido de una trama de Ethernet II. Se utilizará una captura de Wireshark para examinar el contenido de esos campos.

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

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

Paso 2: Examinar la configuración de red de la PC.

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . : udistrital.edu.co
   Descripción . . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Dirección física. . . . . . . . . . . . . : 48-4D-7E-DA-12-2E
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::cbf0:2f89:169d:8670%19(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 10.20.150.217(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.252.0
   Concesión obtenida. . . . . . . . . . . . : miércoles, 24 de septiembre de 2025 6:15:07 a. m.
   La concesión expira . . . . . . . . . . . : miércoles, 24 de septiembre de 2025 8:15:07 a. m.
   Puerta de enlace predeterminada . . . . . : 10.20.150.1
   Servidor DHCP . . . . . . . . . . . . . . : 10.20.110.5
   IAID DHCPv6 . . . . . . . . . . . . . . . : 105401726
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-30-3F-A1-38-48-4D-7E-DA-12-2E
   Servidores DNS. . . . . . . . . . . . . . : 10.20.110.3
                                       10.20.110.5
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

En este caso, la dirección IP de este equipo host es 10.20.150.217, y el gateway predeterminado tiene la dirección IP 10.20.150.1.

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

Primero se realizó el ping a su Gateway predeterminado, para posteriormente evidenciar la respuesta de los paquetes enviados.

```
C:\Users\Estudiantes>ping 10.20.150.1

Haciendo ping a 10.20.150.1 con 32 bytes de datos:
Respuesta desde 10.20.150.1: bytes=32 tiempo<1m TTL=254
Respuesta desde 10.20.150.1: bytes=32 tiempo<1m TTL=254
Respuesta desde 10.20.150.1: bytes=32 tiempo<1m TTL=254
Respuesta desde 10.20.150.1: bytes=32 tiempo<1m TTL=254

Estadísticas de ping para 10.20.150.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

6053	203.893827	Dell_da:8b:9a	Broadcast	ARP	60 Who has 10.20.150.204? Tell 10.20.150.212
6055	204.218226	10.20.150.217	10.20.150.1	ICMP	74 Echo (ping) request id=0x0001, seq=274/4609, ttl=128 (reply in 6056)
6056	204.218611	10.20.150.1	10.20.150.217	ICMP	74 Echo (ping) reply id=0x0001, seq=274/4609, ttl=254 (request in 6055)
6059	204.561882	GProComputer_9d:4c:…	Broadcast	ARP	60 Who has 10.20.150.187? Tell 10.20.150.232
6060	204.604136	Cisco_34:49:df	Broadcast	ARP	60 Who has 10.20.150.190? Tell 10.20.150.1
6061	204.797899	Dell_da:8b:9a	Broadcast	ARP	60 Who has 10.20.150.204? Tell 10.20.150.212
6074	205.224761	10.20.150.217	10.20.150.1	ICMP	74 Echo (ping) request id=0x0001, seq=275/4865, ttl=128 (reply in 6075)
6075	205.225139	10.20.150.1	10.20.150.217	ICMP	74 Echo (ping) reply id=0x0001, seq=275/4865, ttl=254 (request in 6074)
6087	205.408908	GProComputer_9d:4c:…	Broadcast	ARP	60 Who has 10.20.150.187? Tell 10.20.150.232
6090	205.565608	Cisco_34:49:df	Broadcast	ARP	60 Who has 10.20.150.126? Tell 10.20.150.1
6091	205.593892	Cisco_34:49:df	Broadcast	ARP	60 Who has 10.20.150.171? Tell 10.20.150.1
6097	205.810265	Dell_da:8b:9a	Broadcast	ARP	60 Who has 10.20.150.204? Tell 10.20.150.212
6113	206.242271	10.20.150.217	10.20.150.1	ICMP	74 Echo (ping) request id=0x0001, seq=276/5121, ttl=128 (reply in 6114)
6114	206.242662	10.20.150.1	10.20.150.217	ICMP	74 Echo (ping) reply id=0x0001, seq=276/5121, ttl=254 (request in 6113)
6115	206.408938	GProComputer_9d:4c:…	Broadcast	ARP	60 Who has 10.20.150.187? Tell 10.20.150.232
6152	207.259212	10.20.150.217	10.20.150.1	ICMP	74 Echo (ping) request id=0x0001, seq=277/5377, ttl=128 (reply in 6153)
6153	207.259652	10.20.150.1	10.20.150.217	ICMP	74 Echo (ping) reply id=0x0001, seq=277/5377, ttl=254 (request in 6152)
6194	207.633536	Cisco_34:49:df	Broadcast	ARP	60 Who has 10.20.150.192? Tell 10.20.150.1

```
> Frame 38: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{FDFAEB8C-792A-4CAC-96F3-710A7F8EFA4C
v Ethernet II, Src: Dell_da:12:2e (48:4d:7e:da:12:2e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: 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)
  v Source: Dell_da:12:2e (48:4d:7e:da:12:2e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 1]
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Dell_da:12:2e (48:4d:7e:da:12:2e)
    Sender IP address: 10.20.150.217
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.20.150.1
```

```
0000  ff ff ff ff ff ff 48 4d  7e da 12 2e 08 06 00 01   ......HM ~.......
0010  08 00 06 04 00 01 48 4d  7e da 12 2e 0a 14 96 d9   ......HM ~.......
0020  00 00 00 00 00 00 0a 14  96 01                     ........ ..
```

Paso 4: Examinar el contenido del encabezado de Ethernet II de una solicitud de ARP.

Dirección de origen: Dell_da:12:2e (48:4d:7e:da:12:2e)
Tipo de Trama: (0x0806)
Datos: ARP

¿Qué característica significativa tiene el contenido del campo de dirección de destino?
El campo de dirección de destino contiene la dirección de broadcast (ff:ff:ff:ff:ff:ff), lo que significa que la trama se envía a todos los dispositivos de la red local y no a uno en particular.

¿Por qué envía la PC un ARP de difusión antes de enviar la primera solicitud de ping?
La PC envía un ARP de difusión porque necesita conocer la dirección MAC del gateway antes de poder enviar la trama del ping, y como no la tiene registrada en su caché ARP, utiliza una transmisión en broadcast para que el gateway responda con su dirección física.

¿Cuál es la dirección MAC del origen en la primera trama?
Es 48:4d:7e:da:12:2e

¿Cuál es el identificador de proveedor (OUI) de la NIC del origen?
Es Dell (48:4d:7e).

¿Qué porción de la dirección MAC corresponde al OUI?
Es el primer grupo de tres bytes (seis dígitos hexadecimales) de la dirección MAC de origen.

¿Cuál es el número de serie de la NIC del origen?
Es da:12:2e.

PARTE 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

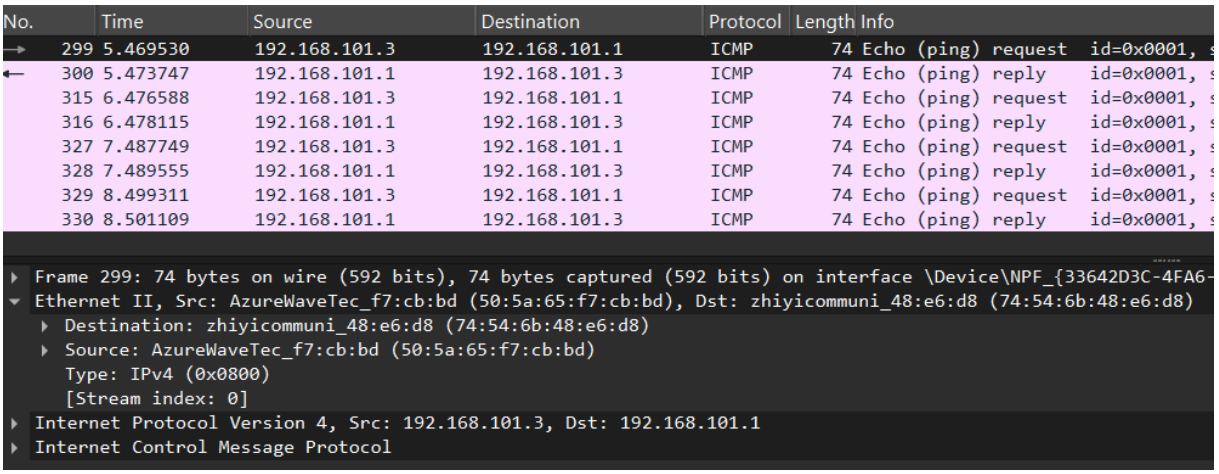
Paso 1: Determinar la dirección IP del gateway predeterminado de la PC.

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . : bbrouter
   Vínculo: dirección IPv6 local. . . : fe80::daae:8dbb:f183:5265%6
   Dirección IPv4. . . . . . . . . . . . : 192.168.101.3
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.101.1
```

¿Cuál es la dirección IP del gateway predeterminado de la PC?
192.168.101.1

Captura al hacer ping al gateway predeterminado de la PC:



¿Cuál es la dirección MAC de la NIC de la PC?
50:5a:65:f7:cb:bd

¿Cuál es la dirección MAC del gateway predeterminado?
74:54:6b:48:e6:d8

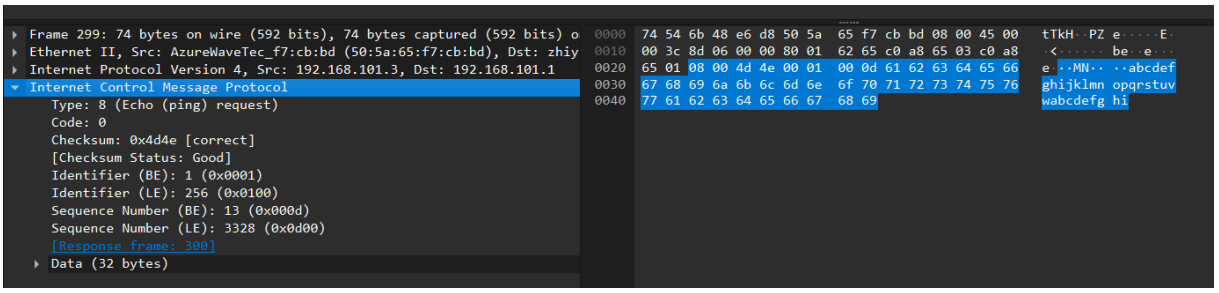
¿Qué tipo de trama se muestra?
El tipo de trama que se muestra es IPv4 (0x0800).

En las últimas dos líneas de la parte central, se proporciona información sobre el campo de datos de la trama. Observe que los datos contienen información sobre las direcciones IPv4 de origen y de destino.

¿Cuál es la dirección IP de origen?
192.168.101.3

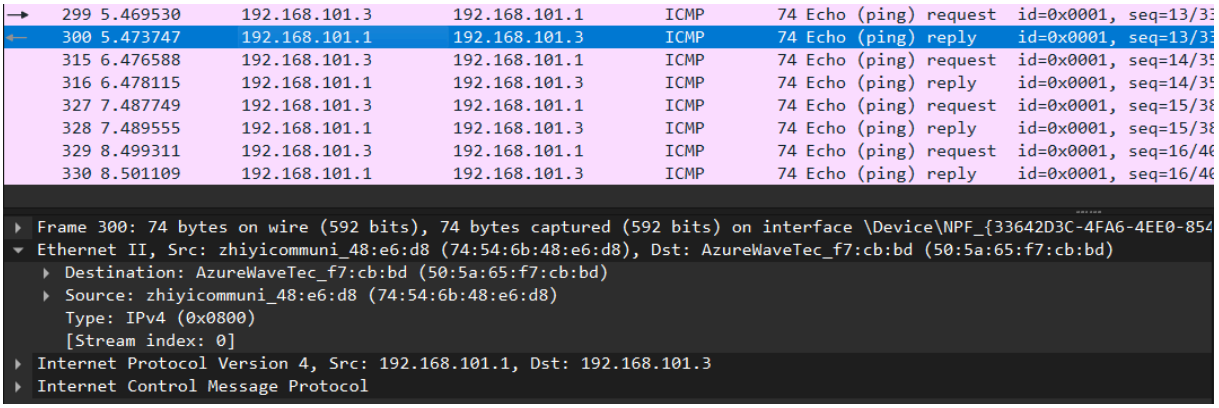
¿Cuál es la dirección IP de destino?
192.168.101.1

Puede hacer clic en cualquier línea de la parte central para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel Packet Bytes de la parte inferior. Haga clic en la línea Internet Control Message Protocol (Protocolo de mensajes de control de Internet) de la parte central y examine lo que se resalta en el panel Packet Bytes.



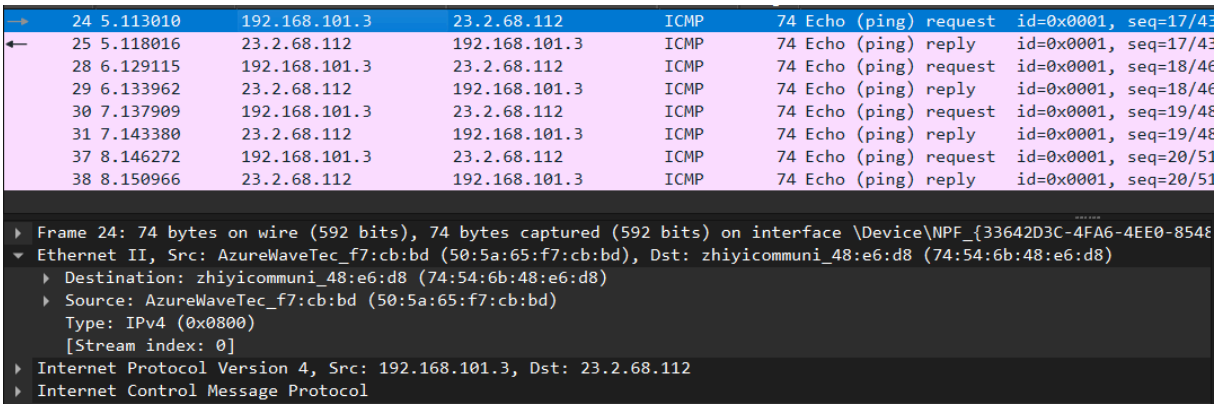
¿Qué texto muestran los últimos dos octetos resaltados?
hi

Haga clic en la siguiente trama de la parte superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y de destino se invirtieron porque esta trama se envió desde el router del gateway predeterminado como respuesta al primer ping.



¿Qué dispositivo y qué dirección MAC se muestran como dirección de destino?
El dispositivo que se muestra en destino es el PC y su dirección MAC 50:5a:65:f7:cb:bd.

Captura al hacer ping a www.cisco.com:



En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y de destino?
Origen: 50:5a:65:f7:cb:bd
Destino: 74:54:6b:48:e6:d8

¿Cuáles son las direcciones IP de origen y de destino que contiene el campo de datos de la trama?
Origen: 192.168.101.3
Destino: 23.2.68.112

Compare estas direcciones con las direcciones que recibió en el paso 6. La única dirección que cambió es la dirección IP de destino. ¿Por qué cambió la dirección IP de destino mientras que la dirección MAC permaneció igual?

Porque ahora el ping se dirigió a un servidor externo diferente al gateway local, pero la dirección MAC de destino se mantuvo igual porque el PC siempre entrega sus tramas al gateway predeterminado. El router es el encargado de encaminar el tráfico hacia la dirección IP final en Internet, pero dentro de la LAN la trama solo necesita llegar a la MAC del gateway.

Reflexión
En Wireshark, no se muestra el campo de preámbulo de un encabezado de trama. ¿Qué contiene el preámbulo?

El preámbulo contiene una serie de bits de sincronización que permiten a los dispositivos prepararse y alinearse para recibir correctamente la trama.

PARTE 2. Visualización de Tablas MAC

Después de configurar las direcciones ip de los PC y los switches, se procede a configurar la contraseña cisco a la consola y de vty, y la contraseña class del modo EXEC privilegiado. A continuación se hace la asignación para el Switch 1.

```
S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#
```

```
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#
```

```
S1(config)#enable password class
S1(config)#exit
S1#
```

Y para el Switch 2.

```
S2>enable
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
```

```
S2(config)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#
```

```
S2(config)#enable password class
S2(config)#exit
S2#
```

Parte 4: Examinar la tabla de direcciones MAC del switch

Paso 1: Registrar las direcciones MAC del dispositivo de red.

Después de configurar las ip de los PC y de los switches, además de agregarles las contraseñas mencionadas, se procede a mirar las MAC de cada equipo, siendo el siguiente resultado para el PC-A

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 000A.F397.9DE0
   Link-local IPv6 Address.........: FE80::20A:F3FF:FE97:9DE0
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-D8-04-1B-69-00-0A-F3-97-9D-E0
   DNS Servers.....................: ::
                                     0.0.0.0
```

Dirección MAC de la PC-A:
000A.F397.9DE0 para el PC-A.

Y para el PC-B:

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0060.5CE7.1BA8
   Link-local IPv6 Address.........: FE80::260:5CFF:FEE7:1BA8
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-28-6A-2D-EA-00-60-5C-E7-1B-A8
   DNS Servers.....................: ::
                                     0.0.0.0
```

Dirección MAC de la PC-B:
0060.5CE7.1BA8

Acceda a los switches S1 y S2 mediante el puerto de consola e introduzca el comando show interface F0/1 en cada switch. En la segunda línea de los resultados del comando, ¿cuáles son las direcciones de hardware (o la dirección física [BIA])?

```
S1#show interface F0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 000b.bec2.0c01 (bia 000b.bec2.0c01)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Dirección MAC Fast Ethernet 0/1 del S1:
000b.bec2.0c01

```
User Access Verification

Password:

S2>enable
Password:
S2#show interface F0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 00d0.ff74.c801 (bia 00d0.ff74.c801)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Dirección MAC Fast Ethernet 0/1 del S2:
00d0.ff.74.c801

Paso 2: Visualizar la tabla de direcciones MAC del switch.
Acceda al switch S2 mediante el puerto de consola y vea la tabla de direcciones MAC antes y después de ejecutar pruebas de comunicación de red con ping.

```
S2#show m
S2#show mac
S2#show mac-a
S2#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000b.bec2.0c01    DYNAMIC     Fa0/1
```

¿Hay direcciones MAC registradas en la tabla de direcciones MAC?
Si, solo una, la del Switch 1.

¿Qué direcciones MAC están registradas en la tabla? ¿A qué puertos de switch están asignadas y a qué dispositivos pertenecen? Omita las direcciones MAC que están asignadas a la CPU.
Esta registrada la dirección 000b.bec2.0c01, asignada al puerto FastEthernet0/1 y pertenece al Switch 1.

Si no registró las direcciones MAC de los dispositivos de red en el paso 1, ¿cómo podría saber a qué dispositivos pertenecen las direcciones MAC utilizando solamente el resultado del comando show mac address-table? ¿Esto funciona en todas las situaciones?
Con el comando show mac address-table solo se puede observar qué direcciones MAC están aprendidas en cada puerto del switch, lo que permite deducir a qué dispositivo pertenece cada dirección únicamente si previamente conocemos qué equipo está conectado a cada puerto, pero esto no siempre funciona en todas las situaciones, ya que en redes más grandes o con cambios de conexión no se puede identificar de manera directa a qué equipo pertenece cada MAC sin información adicional.

Paso 3: Borrar la tabla de direcciones MAC del S2 y volver a visualizar la tabla de direcciones MAC.

En el modo EXEC privilegiado, escriba el comando clear mac address-table dynamic y presione Entrar.

Rápidamente, vuelva a escribir el comando show mac address-table.

```
S2#clear mac address-table dynamic
S2#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000b.bec2.0c01    DYNAMIC     Fa0/1
S2#
```

¿La tabla de direcciones MAC contiene alguna dirección para la VLAN 1? ¿Hay otras direcciones MAC en la lista?
Si, pero únicamente contiene una dirección para la VLAN 1.

Espere 10 segundos, escriba el comando show mac address-table y presione Entrar. ¿Hay nuevas direcciones en la tabla de direcciones MAC?

```
S2#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000b.bec2.0c01    DYNAMIC     Fa0/1
```

No, no aparecen más direcciones MAC.

Paso 4: En la PC-B, hacer ping a los dispositivos en la red y observar la tabla de direcciones MAC del switch.

En la PC-B, abra el símbolo del sistema y escriba arp -a. Sin incluir direcciones de multidifusión o de difusión, ¿cuántos pares de direcciones IP a MAC de dispositivos obtuvo el ARP?

```
C:\>arp -a
No ARP Entries Found
```

Ninguno, debido a que aún no se ha realizado ningún ping.

En el símbolo del sistema de la PC-B, haga ping al S1 y al S2 de la PC-A.
Ping al PC-A:

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping al Switch 1:

```
C:\>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.11: bytes=32 time<1ms TTL=255
Reply from 192.168.1.11: bytes=32 time<1ms TTL=255
Reply from 192.168.1.11: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping al Switch 2:

```
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

¿Todos los dispositivos tuvieron respuestas correctas? De lo contrario, revise el cableado y las configuraciones IP.

Sí, todos los dispositivos respondieron correctamente, aunque en el primer intento se perdió un paquete en la comunicación con los Switches, debido al proceso de resolución ARP, lo cual es normal.

En una conexión de consola al S2, introduzca el comando show mac addresstable.

```
S2#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000a.f397.9de0    DYNAMIC     Fa0/1
   1    000b.bec2.0c01    DYNAMIC     Fa0/1
   1    0060.5ce7.1ba8    DYNAMIC     Fa0/18
```

¿El switch agregó más direcciones MAC a la tabla de direcciones MAC? Si es así, ¿qué direcciones y dispositivos?
Si, agregó dos direcciones más, mostrando un total de tres direcciones.

- 000a.f397.9de0 del PC-A.
- 000b.bec2.0c01 del Switch 1 .
- 0060.5ce7.1ba8 del PC-B.

En la PC-B, abra el símbolo del sistema y vuelva a escribir arp -a.

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.3           000a.f397.9de0        dynamic
  192.168.1.11          000b.be3d.42ab        dynamic
  192.168.1.12          0002.1601.561e        dynamic
```

¿La caché ARP de la PC-B tiene entradas adicionales para todos los dispositivos de red a los que se les hizo ping?
Si, ahora se muestran las direcciones IP y MAC del PC-A, del Switch 1 y del Switch 2.

Reflexión

En las redes Ethernet, los datos se distribuyen a los dispositivos por medio de las direcciones MAC. Para que esto suceda, los switches y las PC arman cachés ARP y tablas de direcciones MAC de manera dinámica. Si la red tiene pocas PC, este proceso parece bastante fácil. ¿Cuáles podrían ser algunos de los desafíos en las redes más grandes?

Algunos de los desafíos que pueden aparecer al tener una red amplia pueden ser el tiempo de respuesta entre la fuente y el receptor, ya que entre mayor cantidad de dispositivos se puede encontrar muchos saltos, lo que a su vez genera más lentitud y posible pérdida de información

o en este caso que el ping no se efectúe de la manera adecuada. Ahora bien, aunque se pudo realizar una comunicación efectiva entre los elementos, se evidenció como los switches se demoraron para realizar su registro de las distintas MAC, por lo que en un red más grande, los switches podrían tener mayor dificultad en definir, encontrar y registrar las direcciones MAC de los dispositivos en la red. Además pensando en la escalabilidad de estos switches, si se le agregan demasiados se puede llegar al punto en que ya no se puedan agregar más y por lo tanto tener un posible límite de dispositivos.

CONCLUSIONES

El uso de Wireshark permitió analizar de manera detallada las tramas Ethernet II, identificando campos clave como las direcciones MAC, el tipo de protocolo encapsulado y las direcciones IP de origen y destino, lo que refuerza la comprensión de la capa de enlace de datos.

De igual forma, se comprobó que el proceso de resolución ARP es indispensable para la comunicación en una red local, y que la pérdida del primer paquete de un ping es un comportamiento normal asociado a la obtención de la dirección MAC del dispositivo de destino.

La práctica con los switches en Packet Tracer permitió observar cómo se construyen dinámicamente las tablas de direcciones MAC, confirmando que estas se van llenando a medida que los dispositivos generan tráfico y que este aprendizaje depende directamente de la interacción en la red.

Además, se evidenció que tanto las tablas MAC de los switches como la caché ARP de los PCs son fundamentales para asegurar el correcto encaminamiento de los datos, y que en redes más grandes este proceso representa un reto mayor en términos de administración y tiempos de respuesta.

Finalmente, el taller permitió integrar la teoría con la práctica demostrando cómo los conceptos de enlace de datos, ARP y tablas MAC se aplican en la operación real de una red, fortaleciendo las bases necesarias para un entendimiento más profundo del funcionamiento y la gestión de las comunicaciones en entornos de red.