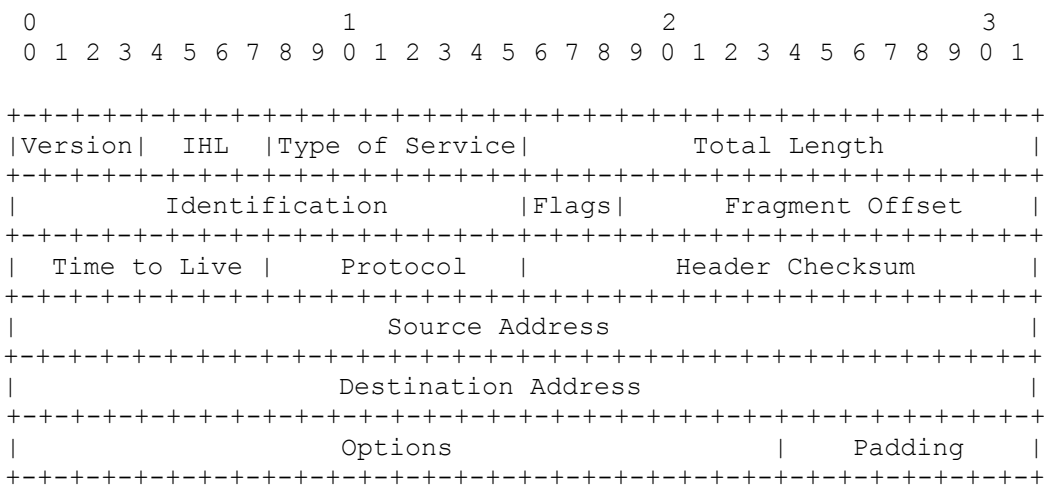
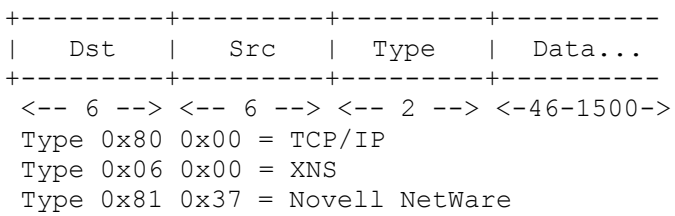
# Analizar las tramas y paquetes de las siguientes direcciones:

**Encabezado IP (Capa de red)**




**Trama Ethernet 2 (Capa de Enlace de Datos)**




1. Análisis de una **IP** de una **máquina de laboratorio**
   a) ¿Cuál es la MAC destino?
   b) ¿Cuál es la IP destino?
   c) En el campo Protocol ¿Cuál es el valor del campo?

2. Análisis de una **IP** de la pagina **www.escom.ipn.mx**
   d) ¿Cuál es la MAC destino?
   e) ¿Cuál es la IP destino?
   f) En el campo Protocol ¿Cuál es el valor del campo?

3. Análisis de una **IP** de la pagina **www.saes.escom.ipn.mx**
   g) ¿Cuál es la MAC destino?
   h) ¿Cuál es la IP destino?
   i) En el campo Protocol ¿Cuál es el valor del campo?

4. Análisis de una **IP 148.204.56.254**
   j) ¿Cuál es la MAC destino?
   k) ¿Cuál es la IP destino?
   l) En el campo Protocol ¿Cuál es el valor del campo?

5. Análisis de una **IP 148.204.61.254**
   m) ¿Cuál es la MAC destino?
   n) ¿Cuál es la IP destino?
   o) En el campo Protocol ¿Cuál es el valor del campo?

6. Análisis de una de la pagina **www.ipn.mx**
   p) ¿Cuál es la MAC destino?
   q) ¿Cuál es la IP destino?
   r) En el campo Protocol ¿Cuál es el valor del campo?

7. Análisis de una de la pagina **www.google.com.mx**
   s) ¿Cuál es la MAC destino?
   t) ¿Cuál es la IP destino?
   u) En el campo Protocol ¿Cuál es el valor del campo?

8. Análisis de una de la pagina **www.facebook.com**
   v) ¿Cuál es la MAC destino?
   w) ¿Cuál es la IP destino?
   x) En el campo Protocol ¿Cuál es el valor del campo?

9. Análisis de una de la pagina **_____**
   y) ¿Cuál es la MAC destino?
   z) ¿Cuál es la IP destino?
   aa) En el campo Protocol ¿Cuál es el valor del campo?

# Uso de Wireshark para examinar las tramas de Ethernet

**Paso 1: Revisar las descripciones y las 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 |

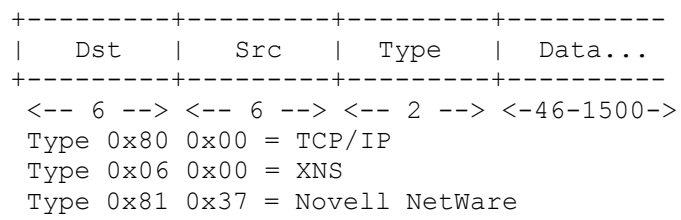
**Paso 4: Examinar el contenido de encabezado de Ethernet II de una solicitud de ARP**

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 II.

| 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`. Un formato común es `12:34:56:78:9A:BC`.<br>Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC); los seis últimos números hexadecimales corresponden al número de serie de la NIC.<br>La dirección de destino puede ser un broadcast, que contiene todos unos, o un unicast. La dirección de origen es siempre unicast. |
| Dirección de origen | Dell_24:2a:60 (5c:26:0a:24:2a:60) | |
| 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 que admite Ethernet II. Dos tipos comunes de trama son:<br>Valor Descripción<br>`0x0800` Protocolo IPv4<br>`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 |

10. Capturar una trama ARP (mandar un ping a la **IP 148.204.56.255**) y rellenar los campos

**Trama Ethernet 2 (Capa de Enlace de Datos)**




**Reflexión**

11. ¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos?

12. ¿Cuál es la importancia del análisis de una red con el programa Wireshark?