

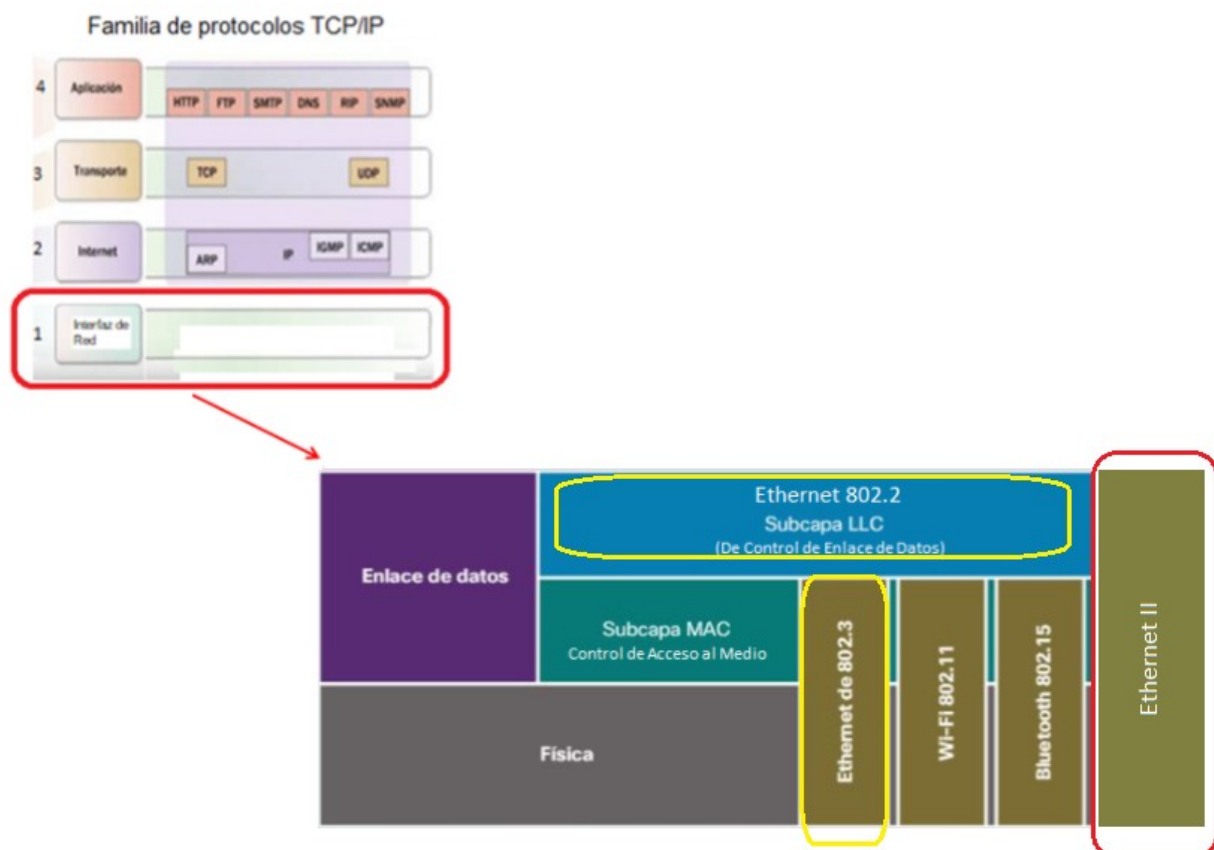
Unidad 6. Direcccionamiento de Hardware, Tipo de Cuadro, Capa Interfaz de Red. **(Capa 1)**

TEMA 1. Dirección Física o MAC, Control de Acceso al Medio.

TEMA 2. Estructura de Trama de Protocolo Ethernet II. Campos de la Trama. Concepto de Difusión.

TEMA 3. Norma Ethernet II y su evolución a Normas 802.2 y 802.3.

TEMA 4. Analizadores de Tráfico de Red, también llamados Monitores de Red y Sniffers.



TEMA 1. Dirección Física o MAC, Control de Acceso al Medio.

F1:4A:C2:FF:1B:CC

IEEE

/

FABRICANTE

En redes de computadores, la dirección MAC, Control de Acceso al Medio, es un identificador hexadecimal de 6 bytes, 48 bits, que se corresponde de forma única con una tarjeta de interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y que es configurada por el organismo IEEE en sus primeros 24 bits y por el fabricante de la Interfaz de red los 24 bits restantes.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos

Se expresa en el Sistema Hexadecimal, cada byte separado por dos puntos, por ejemplo:

F1:4A:C2:FF:1B:CC

Son seis octetos o bytes de ocho bits cada uno, separados por dos puntos, expresados en el Sistema Hexadecimal.

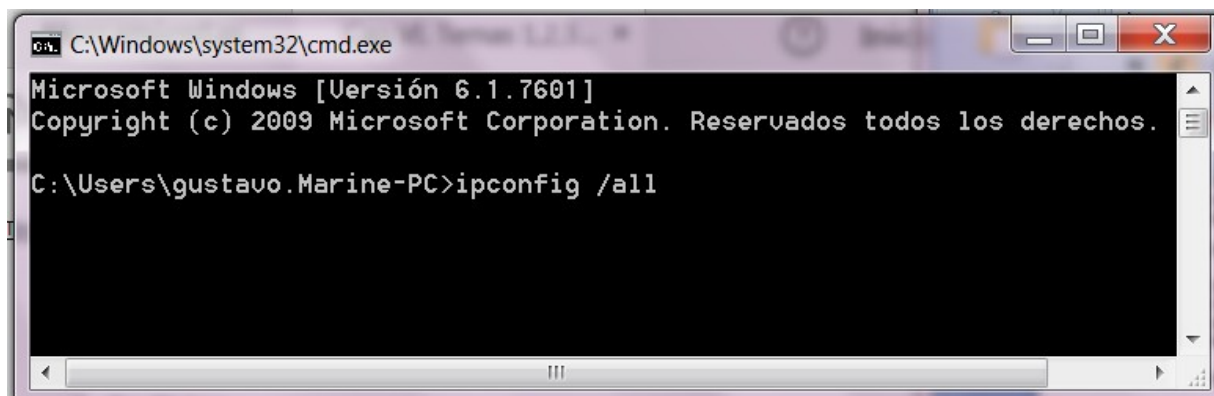
Para conocer cuál es la dirección MAC de un equipo hay que proceder de la siguiente forma.

1. Para Windows.

Ir a ----- **Inicio** ---- **Ejecutar**

En el cuadro que aparece, que nos permite buscar programas, teclear ---- **cmd** -----
Enter

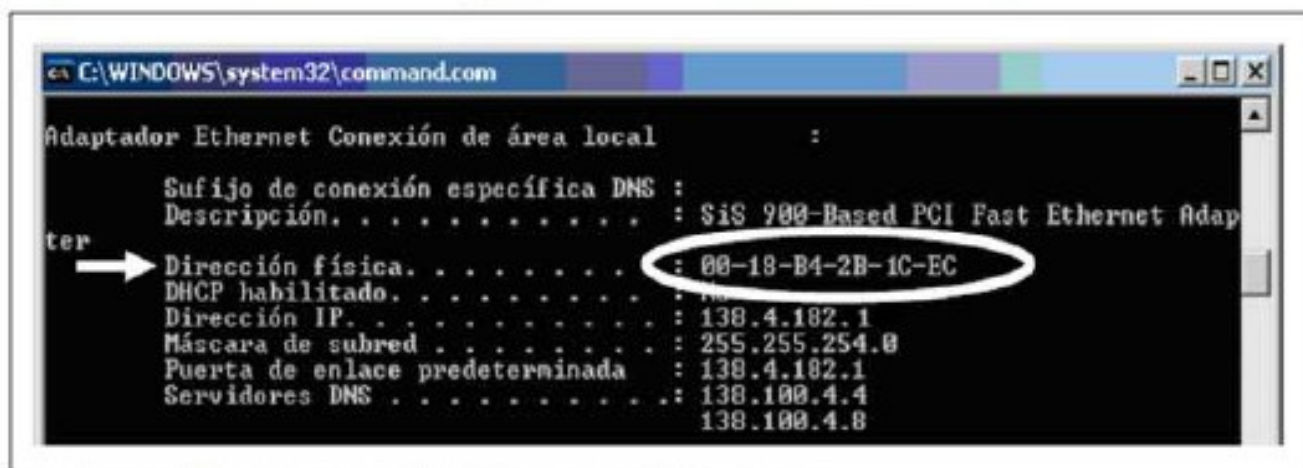
Se abrirá una pantalla de DOS, como la siguiente, en ella escribir ----- **ipconfig /all** --- **Enter**



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\gustavo.Marine-PC>ipconfig /all
```

De esta forma obtendremos una serie de parámetros relacionados con la configuración de red, entre ellos la dirección MAC, que aparece en la siguiente imagen marcada con un círculo.

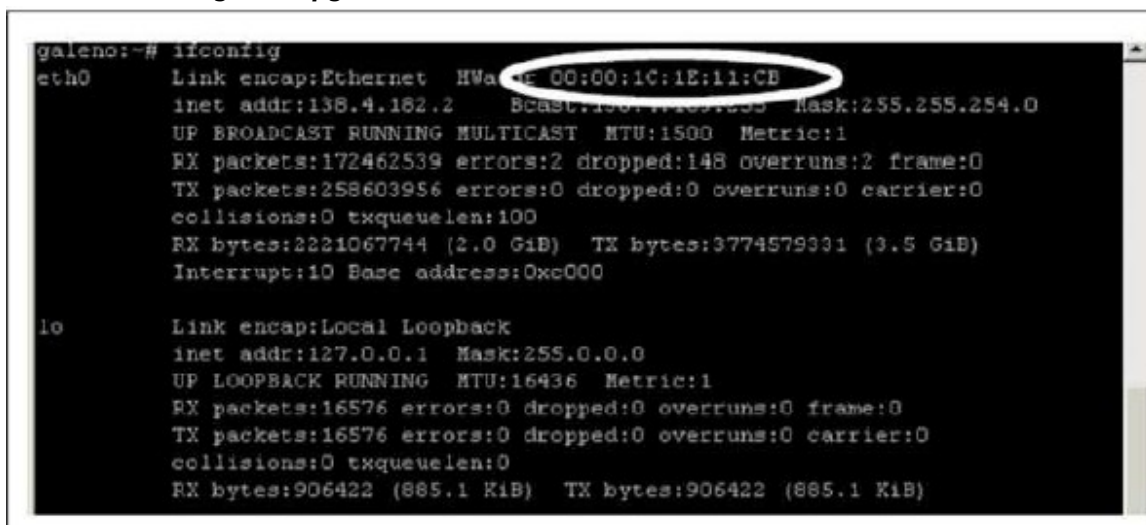


```
C:\WINDOWS\system32\command.com

Adaptador Ethernet Conexión de área local :
Sufijo de conexión específica DNS :
Descripción. . . . . : SiS 900-Based PCI Fast Ethernet Adap
ter → Dirección física. . . . . : 00-18-B4-2B-1C-EC
DHCP habilitado. . . . . : No
Dirección IP. . . . . : 138.4.182.1
Máscara de subred . . . . . : 255.255.254.0
Puerta de enlace predeterminada : 138.4.182.1
Servidores DNS . . . . . : 138.100.4.4
                          : 138.100.4.8
```

2. Para Linux / Unix.

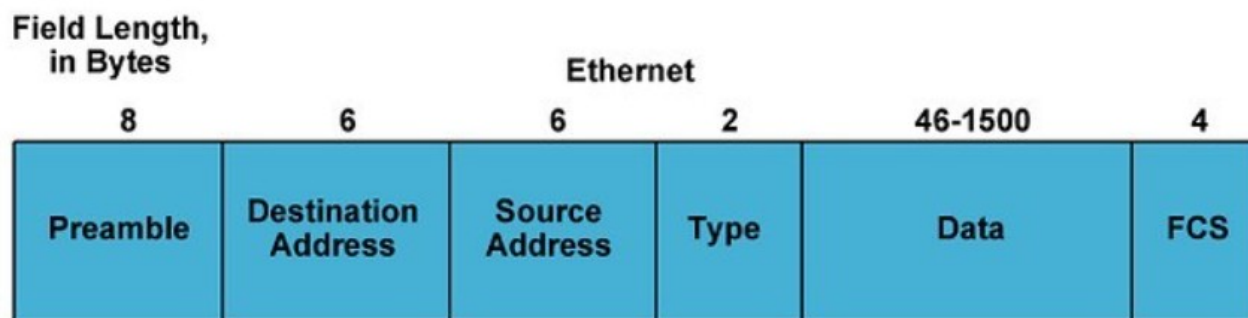
Una vez ingresada a la Terminal de Linux hay que teclear: **ifconfig** y encontraremos la MAC como muestra la siguiente figura.



```
galeno:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:00:1C:1E:11:CB
          inet addr:138.4.182.2  Bcast:138.4.182.255  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:172462539 errors:2 dropped:148 overruns:2 frame:0
          TX packets:258603956 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2221067744 (2.0 GiB)  TX bytes:3774579331 (3.5 GiB)
          Interrupt:10 Base address:0xc000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16576 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16576 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:906422 (885.1 KiB)  TX bytes:906422 (885.1 KiB)
```

TEMA 2. Estructura de Trama en Norma Ethernet II. Concepto de Difusión en Capa Interfaz de Red.



La Estructura del Protocolo ETHERNET II, está conformada por los siguientes campos:

PREÁMBULO, 8 bytes.

Este primer campo está constituido siempre por una secuencia alternada de unos y cero, lo cual permite la sincronización entre el computador Transmisor y los computadores Receptores.

DIRECCIÓN DESTINO, 6 bytes.

El segundo Campo contiene la Dirección Física, MAC, del computador Receptor, es decir la MAC del computador a quien está destinado el envío de esta Trama.

Todos los computadores de la red reciben la Trama enviada por el computador Transmisor. El computador que recibe la trama compara la Dirección Destino de la Trama, es decir este campo, con su propia Dirección Física, MAC. Si coinciden confirma que la Trama es dirigida a ella y la toma. Si no coinciden la descarta.

Existen dos tipos de Direcciones de Destino soportadas:

1. **Individual**, El campo de Dirección Destino contiene una dirección única e individual que corresponde a un computador de la Red. También llamada **Unicast**.
2. **Difusión, (Broadcast o Multicast)**. En la cual la Dirección Destino está conformada completamente por una secuencia de unos. En hexadecimal se expresa de la siguiente manera:

Binario 1111 1111 1111 1111 1111 1111 1111 1111

Binario a Hexadecimal F F F F F F F F

Hexadecimal FF:FF:FF:FF:FF:FF

Si la Trama está compuesta por la Dirección de Difusión, llamada también Dirección de Broadcast, o Dirección de Multicast, todos los computadores de la Red donde se originó la difusión están obligados a tomar la Trama.

Esta forma de Transmisión se utiliza cuando un computador necesita enviar un mensaje a todos los otros, por ejemplo cuando se quiere enviar un mensaje de alerta por algún evento especial que involucra a todos los computadores. Por ejemplo un mensaje de aviso porque se va a reiniciar un computador Servidor.

DIRECCIÓN FUENTE, 6 bytes.

Este campo es provisto por la MAC del computador Transmisor, el cual inserta su propia dirección MAC, indicando que es la estación Originadora o Fuente de la Transmisión.

TIPO, 2 bytes.

Este campo se denomina TIPO en la norma Ethernet II de la capa de Interfaz de Red, (Capa 1), e indica el Tipo de datos de la Capa superior, (capa de Internet), que son transportados por la Trama, por ejemplo: Tipos de datos IP, IPX, ICMP, todos ellos correspondientes a la Capa de Internet, (Capa 2). En este caso el campo de Tipo se denomina explícito.

DATOS, 46 a 1500 bytes.

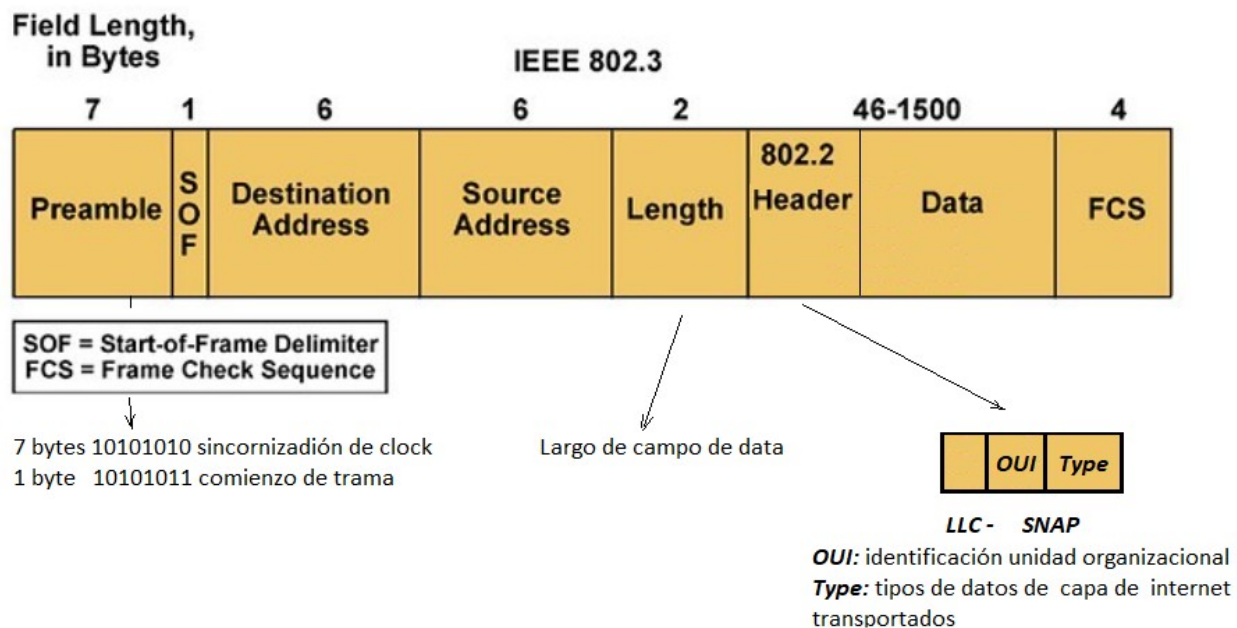
Este Campo contiene los datos, es decir la información útil a ser transferida. Tiene un límite máximo y un límite mínimo. El límite mínimo es el mínimo necesario para que pueda ejecutarse correctamente la Comprobación de Redundancia Cíclica, CRC, que permite la comprobación de la Trama. El CRC se incluye en el último Campo de la Trama.

CRC, Comprobación de Redundancia Cíclica, también llamado FCS, Secuencia de Chequeo de Trama, 4 bytes.

Este Campo contiene el valor del algoritmo obtenido por el CRC con la operación realizada con la Trama Completa. El CRC es una operación matemática realizada por el computador Transmisor y en la cual intervienen todos los campos de la trama, Dirección Destino, Dirección Fuente, Tipo/Longitud y Datos, y el mismo es anexado en los últimos cuatro bytes de la Trama.

El computador Receptor ejecuta también la operación matemática y comprueba el resultado con el valor llegado en el campo de CRC de la trama. De esta forma se conforma el Sistema de Detección de Errores para descartar Tramas Corruptas con información alterada.

TEMA 3. Norma Ethernet II y su evolución a Normas 802.2 y 802.3. Subcapas ,Snap y LLC.



La diferencia más significativa entre la Norma Ethernet II original y la Norma IEEE 802.3 es la diferencia entre los formatos de sus tramas. Esta diferencia es lo suficientemente significativa como para hacer a las dos versiones incompatibles.

Una de las diferencias entre el formato de las dos tramas está en el preámbulo. El propósito del preámbulo es anunciar la trama y permitir a todos los receptores en la red sincronizarse a la trama entrante.

El preámbulo en Ethernet II tiene una longitud de 8 bytes pero en IEEE 802.3 la longitud del mismo es de 7 bytes, y el octavo byte se convierte en el delimitador de la trama.

La segunda diferencia entre el formato de las tramas es en el campo Tipo que se encuentra en la norma Ethernet II. El campo de Tipo es usado para especificar el protocolo de la Capa de Internet, (Capa 2), que es transportado en la trama. Esto posibilita que muchos protocolos de Capa 3 puedan ser transportados en la trama.

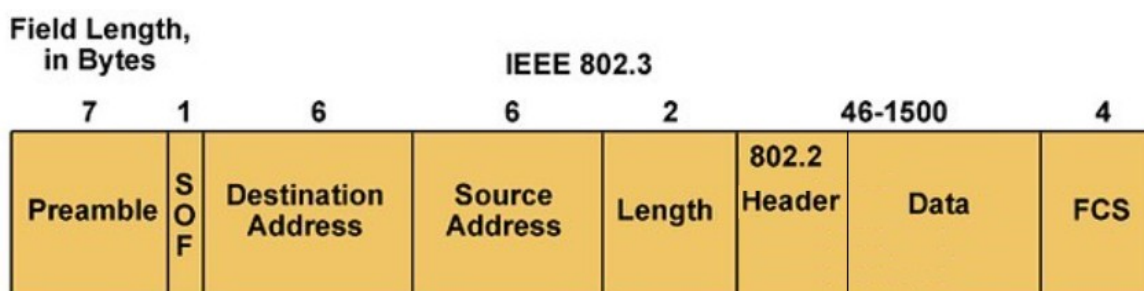
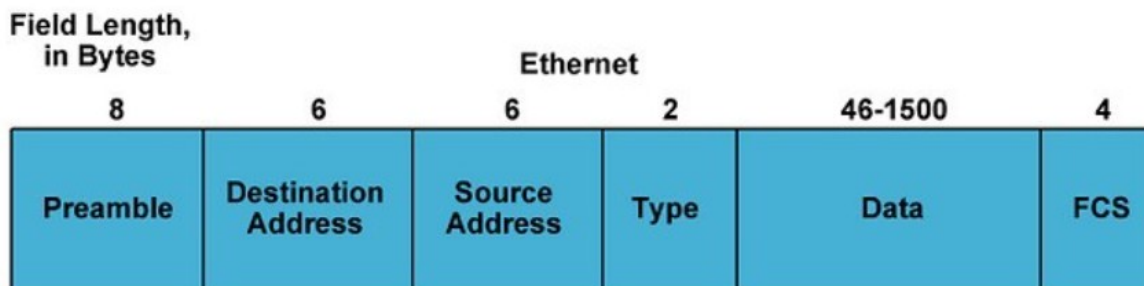
El campo de Tipo fue reemplazado en la norma IEEE 802.3 por un campo denominado LONGITUD, que indica la Longitud del siguiente campo, el Campo de Datos. La Cabecera de Tipo se encuentra incorporada en los primeros bytes del Campo de Datos. En este caso el campo de Tipo se denomina implícito porque se encuentra oculto en los primeros bytes del campo de Datos.

La Norma Ethernet II define un Campo de Tipo explícito, perfectamente delimitado ya que consta de 2 bytes, pero también limitado con respecto al crecimiento de los futuros Tipos de Cuadros.

La Norma 802.3 define un Campo de Tipo implícito, incluido en los primeros bytes del Campo de Datos. Esto permite la creación de nuevos tipos de datos, ya que posee un campo que identifica la organización que creó el tipo de dato y otro campo donde se especifica el tipo de dato creado por esa organización.

Esta cabecera se llama: cabecera LLC/SNAP y fue totalmente definida por la norma 802.2.

LLC/SNAP: Control de Enlace Lógico / Punto de Acceso de Subred.



SOF = Start-of-Frame Delimiter
FCS = Frame Check Sequence

7 bytes 10101010 sincronización de clock
1 byte 10101011 comienzo de trama

Largo de campo de data



LLC - SNAP

OUI: identificación unidad organizacional
Type: tipos de datos de capa de internet transportados

Tipos de datos de capa de Internet transportados.

Hexadecimal	Significado
0800	IPv4 de TCP/IP.
8137-8138	IPX de Novell Co.
6559	Frame Relay. Wan.
809B	Apple Talk de Apple Co.

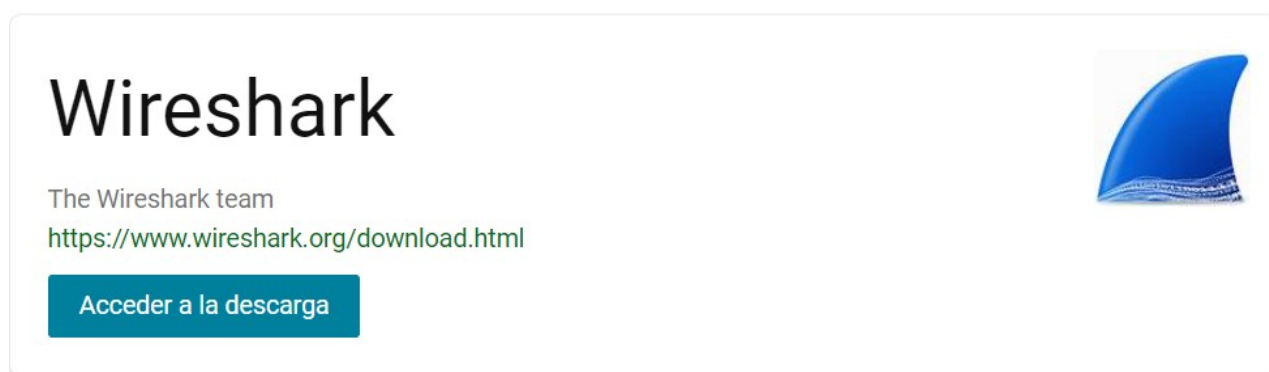
Una diferencia entre el formato de las dos tramas está en el *preámbulo*. El propósito del preámbulo es anunciar la trama y permitir a todos los receptores en la red sincronizarse a sí mismos a la trama entrante. El preámbulo en Ethernet es una longitud de *8 bytes* pero en IEEE 802.3 la longitud del mismo es de *7 bytes*. En este último el octavo byte se convierte en el comienzo del delimitador de la trama. (SOF: Start of Frame, comienzo de trama).

La segunda diferencia entre el formato de las tramas está en el campo *tipo de trama* que se encuentra en la trama Ethernet. Un campo tipo es usado para especificar el protocolo que es transportado en la trama. Esto posibilita que muchos protocolos puedan ser transportados en la trama. El campo tipo fue reemplazado en el estándar 802.3 por un campo *longitud de trama*, el cual es utilizado para indicar el número de bytes que se encuentra en el campo de los datos.

La tercera diferencia entre el formato de las tramas está en los campos de *dirección*, tanto de *destino* como de *origen*. Mientras que en el formato de **IEEE 802.3 permite el uso tanto de direcciones de 2 bytes como de 6 bytes, el estándar Ethernet permite direcciones de 6 bytes.**

El formato de trama que predomina actualmente en los ambientes Ethernet es el de IEEE 802.3, pero aún se continúa utilizando en algunos casos la Norma Ethernet original, por eso las interfaces de red levantan los dos protocolos para ser utilizados según la ocasión.

TEMA 4. Analizadores de Tráfico de Red, también llamados Monitores de Red y Sniffers.



Un Analizador de Tramas es una Aplicación de captura de las tramas que circulan por una Red de computadores.

Todas las Redes de Área Local, (Redes Lans), cualquiera sea el medio utilizado para la transmisión, (cable coaxial, cable de par trenzado, fibra óptica, etc), utilizan el mismo sistema llamado canal compartido.

El canal compartido por todos los computadores de la red hace posible que un ordenador especializado, capture todas las tramas de información que viajan por la red.

Este computador especializado puede capturar todas las tramas de información, inclusive las que no están destinadas a él. Esto es lo que hace un computador que tiene instalada una Aplicación llamada "Analizador de Tráfico de Tramas". Para conseguir esto el Analizador configura la Interfaz de Red o Tarjeta de Red en un estado conocido como "Modo Promiscuo", mediante el cual ninguna trama es descartada, cualquiera sea la dirección MAC destino de la trama.

De esta manera se puede capturar, todo el tráfico que viaja por la red. El Analizador o Monitor de Red, llamado también Sniffer, (Sniff: olfatear en inglés), es una Aplicación que permite determinar el nivel

de desempeño de una red. De esta forma captura las tramas, analiza los campos de las mismas y genera estadísticas.

Por ejemplo:

1. Cantidad promedio de tramas por segundos.
2. Tamaño promedio de las tramas.
3. Cantidad de colisiones que se producen en el período de captura.
4. En la Red Token Ring puede comunicar el Retardo promedio de la Ficha.
5. Cantidad de tramas enviadas por un computador durante el período de captura.
6. Cantidad de tramas recibidas por un computador durante el período de captura.
7. Se pueden observar y analizar los cuadros enviados por un computador particular, observando el tráfico de cierto tipo, o calcular el porcentaje de cuadros de cada tipo.

El Analizador examina los campos de la cabecera y mediante la configuración que selecciona el usuario, determina los resultados a mostrar.

Por ejemplo, si se desconfía de un computador, conociendo su Dirección Física, MAC address, se puede configurar el Analizador para presentar todos los cuadros que se originan en él. El Analizador retendrá todas las tramas que tengan en el Campo de Dirección Fuente de la cabecera, el valor de la Dirección Física del computador investigado.


Ejemplo de Sniffer WireShark:

Wireshark

The Wireshark team

<https://www.wireshark.org/download.html>

Acceder a la descarga



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
13	5.061810	192.168.100.19	172.217.162.3	ICMP	74	Echo (ping) request id=0x0001, seq=1045/5380, ttl=128 (reply in 14)
14	5.082944	172.217.162.3	192.168.100.19	ICMP	74	Echo (ping) reply id=0x0001, seq=1045/5380, ttl=56 (request in 13)
15	6.066766	192.168.100.19	172.217.162.3	ICMP	74	Echo (ping) request id=0x0001, seq=1046/5636, ttl=128 (reply in 16)
16	6.087404	172.217.162.3	192.168.100.19	ICMP	74	Echo (ping) reply id=0x0001, seq=1046/5636, ttl=56 (request in 15)

> Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 > Ethernet II, Src: IntelCor_ba:79:67 (34:41:5d:ba:79:67), Dst: HuaweiTe_96:d8:8c (14:57:9f:96:d8:8c)
 > Internet Protocol Version 4, Src: 192.168.100.19, Dst: 172.217.162.3
 > Internet Control Message Protocol

MAC Destino MAC Origen Tipo

```

0000 14 57 9f 96 d8 8c 34 41 5d ba 79 67 08 00 45 00  .W....4A ).yg.dE-
0010 00 3c 37 eb 00 00 80 01 8f 3d c0 a8 64 13 ac d9  -<7....-...d...
0020 a2 03 08 00 49 45 00 01 04 16 61 62 63 64 65 66  -...IE...-abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```