ARP

El protocolo ARP es un protocolo estándar específico de las redes. Su status es electivo.

El protocolo de resolución de direcciones es responsable de convertir las dirección de protocolo de alto nivel(direcciones IP) a direcciones de red físicas. Primero, consideremos algunas cuestiones generales acerca de Ethernet.

ARP se emplea en redes IEEE 802 además de en las viejas redes DIX Ethernet para mapear direcciones IP a dirección hardware. Para hacer esto, ha de estar estrechamente relacionado con el manejador de dispositivo de red. De hecho, las especificaciones de ARP en RFC 826 sólo describen su funcionalidad, no su implementación, que depende en gran medida del manejador de dispositivo para el tipo de red correspondiente, que suele estar codificado en el microcódigo del adaptador.

Si una aplicación desea enviar datos a una determinado dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un "router") y el dispositivo hardware al que se debería enviar. Si se trata de una red 802.3/4/5, deberá consultarse el módulo ARP para mapear el par <tipo de protocolo, dirección de destino> a una dirección física.

El módulo ARP intenta hallar la dirección en su caché. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador(el manejador de dispositivo). Si no lo encuentra, descarta el paquete (se asume que al ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP.

ARP y subredes

El protocolo ARP es el mismo aunque haya subredes. Recordar que cada datagrama IP pasa primero por el algoritmo de encaminamiento IP. Este algoritmo selecciona el manejador de dispositivo que debería enviar el paquete. Sólo entonces se consulta al módulo ARP asociado con ese manejador.

IP

Un protocolo es un conjunto de normas que rigen el funcionamiento de las cosas en una determinada tecnología, por lo que de esta forma se consigue que exista algún tipo de estandarización. Cuando hablamos de comunicaciones de red, un protocolo es el conjunto de normas que rigen cómo los paquetes de comunicación se transmiten a través de la red. Cuando tienes un protocolo, puedes estar seguro de que todas las máquinas de una red (o del mundo, cuando se trata de Internet), por muy diferentes que sean, hablan el mismo idioma y pueden integrarse en cualquier sistema.

Desarrollado durante la década de 1970, el protocolo IP es el protocolo de red fundamental usado a través de Internet, las redes domésticas y las redes empresariales. El protocolo IP se utiliza a menudo junto con el protocolo de control de transporte (Transport Control Protocol o TCP) y entonces se les llama de manera intercambiable tanto protocolo IP como protocolo TCP/IP.

IPv4 e IPv6

La mayoría de las redes utilizan el estándar de protocolo IP versión 4 (IPv4) que cuenta con direcciones IP de cuatro bytes (32 bits) de longitud. Desde hace tiempo se sabe que con el aumento de dispositivos conectados a Internet, los 4 bytes de este protocolo no son suficientes y es necesario mejorarlo. La versión 6 del protocolo IP (IPv6), diseñada para sustituir a IPv4, tiene direcciones IP de 16 bytes (128 bits) de longitud.

Hay gente que tiene curiosidad por saber qué pasó con la versión del protocolo que se queda en medio, la hipotética IPv5. La realidad es que IPv5 nunca ha sido un protocolo oficial. Hace unos años, Internet Stream Protocol (ST) fue considerado como la versión 5 por algunos investigadores, pero ST fue abandonado antes de llegar a ser un estándar. Nunca fue conocido como IPv5. Y no se espera que el trabajo en ST y IPv5 se reinicie nunca.

¿Cómo funciona el protocolo IP?

Los datos en el protocolo IP están organizados en mensajes. Estos mensajes se denominan muchas veces paquetes y algunas veces datagramas, pero en términos sencillos todos ellos se refieren más o menos al mismo concepto. Cada datagrama IP incluye tanto una cabecera (que especifica origen, destino, y otra información acerca de los datos) como los propios datos del mensaje.

Los datagramas IP

Como hemos dicho, cada datagrama IP incluye tanto una cabecera (que especifica origen, destino, y otra información acerca de los datos) como los propios datos del mensaje. IP utiliza una cabecera base de 20 bytes (5 palabras) de longitud, con opciones de encabezado expandido adicionales, seguido de los datos.

Las 5 palabras de las cabeceras IP contienen:

Palabra 1:

Versión del Protocolo de Internet utilizado (por ejemplo IPv4)

IHL: Longitud de la cabecera

DSCP: Punto de código de servicios diferenciados. Este es el tipo de servicio

ECN: Notificación de congestión explícita. Lleva información sobre la congestión en la ruta.

Longitud total: Longitud de paquete IP

Palabra 2:

Identificación: Si paquete IP está fragmentado durante la transmisión, todos los fragmentos contienen el mismo número de identificación original

Flags de fragmentación: si el paquete IP es demasiado grande estos flags indican si se puede fragmentar o no.

Flags de desplazamiento: este desplazamiento indica la posición exacta del fragmento en el paquete IP original

Palabra 3:

Tiempo de vida (TTL): Para evitar bucles, cada paquete es enviado con un valor de TTL que indica a la red el número de routers (saltos) que este paquete puede cruzar. En cada salto, su valor se decrementa en uno y cuando el valor llega a cero, el paquete se descarta.

Protocolo de Transporte: Indica la capa de red en el host de destino.

Checksum del encabezado: Este campo se usa para comprobar si el paquete es recibido sin error.

Palabra 4:

Dirección de Origen: dirección de 32 bits del remitente (o fuente) del paquete.

Palabra 5:

Dirección de destino: dirección de 32 bits del receptor (o destino) del paquete.

Opciones: Este campo es opcional y puede contener valores para opciones tales como la seguridad, Ruta de registro, la marca de tiempo, etc.

La carga útil de un datagrama IP pueden ser de longitud variable. El tamaño mínimo de un datagrama IP es de 28 bytes, utilizando el mínimo de 20 bytes de información de cabecera, seguido por el mínimo de 8 bytes de datos. El tamaño máximo de un datagrama IP es de 65.535 bytes menos el tamaño de la cabecera.Tramas

{//t1

0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0x00, 0x23, 0x8b, 0x46, 0xe9, 0xad, 0x08, 0x06, 0x00, 0x10, 0x08, 0x00, 0x06, 0x04, 0x00, 0x04, 0x00, 0x23, 0x8b, 0x46, 0xe9, 0xad, 0x94, 0xcc, 0x39, 0xcb, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x94, 0xcc, 0x39, 0xfe

},

{//t2

0x00, 0x1f, 0x45, 0x9d, 0x1e, 0xa2, 0x00, 0x23, 0x8b, 0x46, 0xe9, 0xad, 0x08, 0x00, 0x46, 0x00, 0x80, 0x42, 0x04, 0x55, 0x34, 0x11, 0x80, 0x11, 0x6b, 0xf0, 0x94, 0xcc, 0x39, 0xcb, 0x94, 0xcc, 0x67, 0x02, 0xaa, 0xbb, 0xcc, 0xdd, 0x04, 0x0c, 0x00, 0x35, 0x00, 0x2e, 0x85, 0x7c, 0xe2, 0x1a, 0x01, 0x00, 0x00, 0x01, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x03, 0x77, 0x77, 0x77, 0x03, 0x69, 0x73, 0x63, 0x05, 0x65, 0x73, 0x63, 0x6f, 0x6d, 0x03, 0x69, 0x70, 0x6e, 0x02, 0x6d, 0x78, 0x00, 0x00, 0x1c, 0x00, 0x01

},

{//t3

0x00, 0x02, 0xb3, 0x9c, 0xdf, 0x1b, 0x00, 0x02, 0xb3, 0x9c, 0xae, 0xba, 0x00, 0x04, 0xf0, 0xf1, 0x09, 0x8d, 0x00, 0x7c, 0x9b, 0x6d

},

{//t4

0x00, 0x23, 0x8b, 0x46, 0xe9, 0xad, 0x00, 0x1f, 0x45, 0x9d, 0x1e, 0xa2, 0x80, 0x35, 0x00, 0x01, 0x08, 0x00, 0x06, 0x04, 0x00, 0x03, 0x00, 0x1f, 0x45, 0x9d, 0x1e, 0xa2, 0x94, 0xcc, 0x3a, 0xe1, 0x00, 0x23, 0x8b, 0x46, 0xe9, 0xad, 0x94, 0xcc, 0x39, 0xcb, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0xd8, 0xee, 0xdf, 0xb0

},

{//t5

0x00, 0x02, 0xb3, 0x9c, 0xae, 0xba, 0x00, 0x02, 0xb3, 0x9c, 0xdf, 0x1b, 0x00, 0x03, 0xf0, 0xf0, 0x53, 0x00, 0x43, 0x05, 0x90, 0x6d

},

{//T6

0x00, 0x02, 0xb3, 0x9c, 0xae, 0xba, 0x00, 0x02, 0xb3, 0x9c, 0xdf, 0x1b, 0x00, 0x12, 0xf0, 0xf0, 0x0a, 0x0b,
0x0e, 0x00, 0xff, 0xef, 0x14, 0x00, 0x00, 0x00, 0x28, 0x00, 0x00, 0x00, 0x7f, 0x23, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x01, 0x99, 0x98, 0x6d

},

{//t7

0x00, 0x02, 0xb3, 0x9c, 0xae, 0xba, 0x00, 0x02, 0xb3, 0x9c, 0xdf, 0x1b, 0x00, 0x03, 0xf0, 0xf1, 0x53, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x43, 0x05, 0x90, 0x6d

},

{ //t8

0x00, 0x02, 0xb3, 0x9c, 0xae, 0xba, 0x00, 0x02, 0xb3, 0x9c, 0xdf, 0x1b, 0x00, 0x03, 0xf0, 0xf0, 0x43, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x43, 0x05, 0x90, 0x6d

}

{//t9

0x1f,0x45,0x9d,0x1e,0xa2,0x00,0x23,0x8b,0x46,0xe9,0xad,0x08,0x00,0x45,0x10,0x3c,0x04,0x57,0x00,0x00,
0x80,0x01,0x98,0x25,0x94,0xcc,0x39,0xcb,0x94,0xcc,0xe1,0x08,0x00,0x49,0x5c,0x03,0x00,0x01,0x00,0x61,
0x62,0x63,0x64,0x65,0x66,0x68,0x69,0x6a,0x6b,0x6c,0x6d,0x6e,0x6f,0x70,0x71,0x72,0x73,0x74,0x75,0x76,
0x61,0x62,0x63,0x64,0x65,0x66,0x67,0x68,0x69

},

{//10

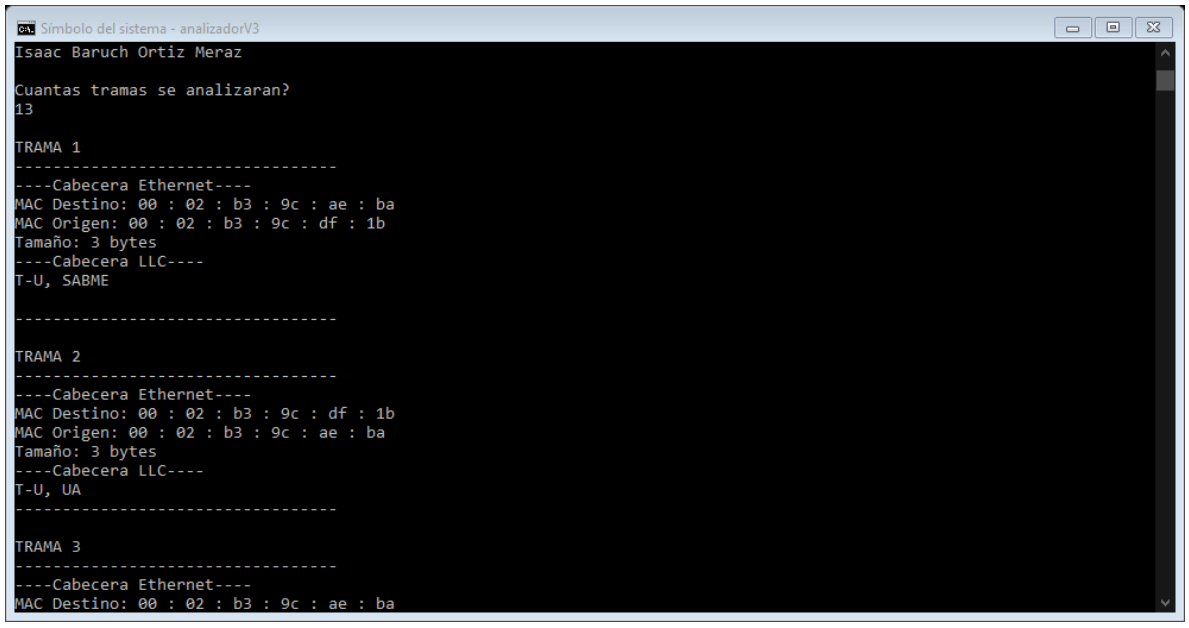
0x00,0x1f,0x45,0x9d,0x1e,0xa2,0x00,0x23,0x8b,0x46,0xe9,0xad,0x08,0x00,0x46,0x08,0x80,0x42,0x04,0x55,
0x34,0x11,0x80,0x11,0x6b,0xf0,0x94,0xcc,0x39,0xcb,0x94,0xcc,0x67,0x02,0xaa,0xbb,0xcc,0xdd,0x04,0x0c,0
x00,0x35,0x00,0x2e,0x85,0x7c,0xe2,0x1a,0x01,0x00,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x03,0x77,0
x77,0x77,0x03,0x69,0x73,0x63,0x05,0x65,0x73,0x63,0x6f,0x6d,0x03,0x69,0x70,0x6e,0x2,0x6d,0x78,0x00,0x
00,0x1c,0x00,0x01},

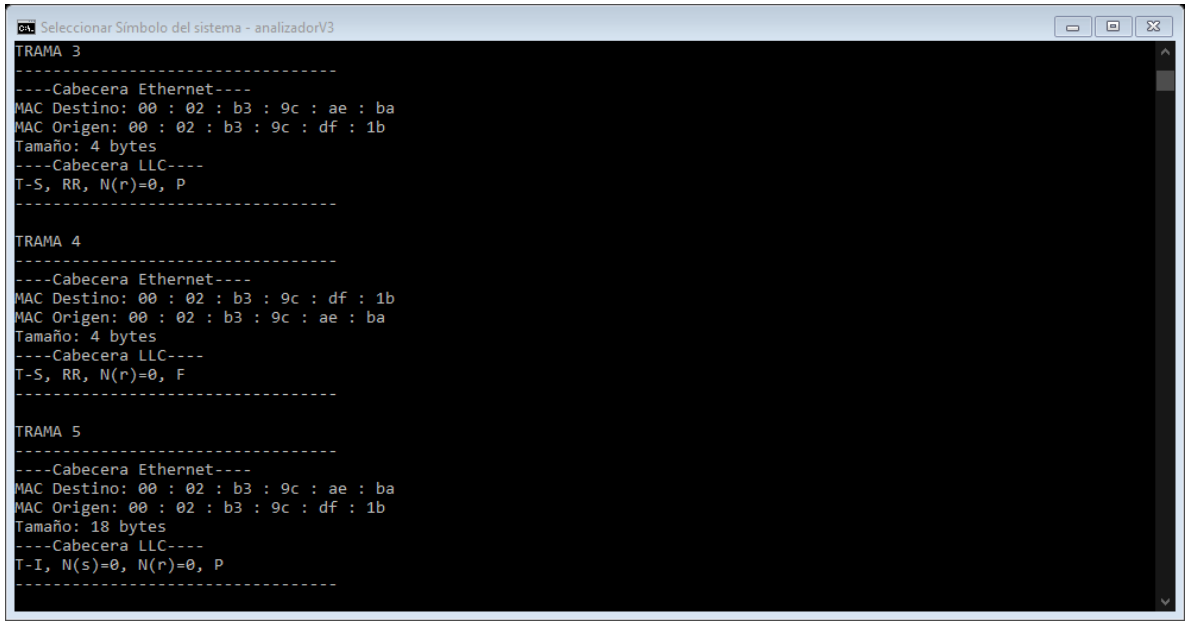
{//11

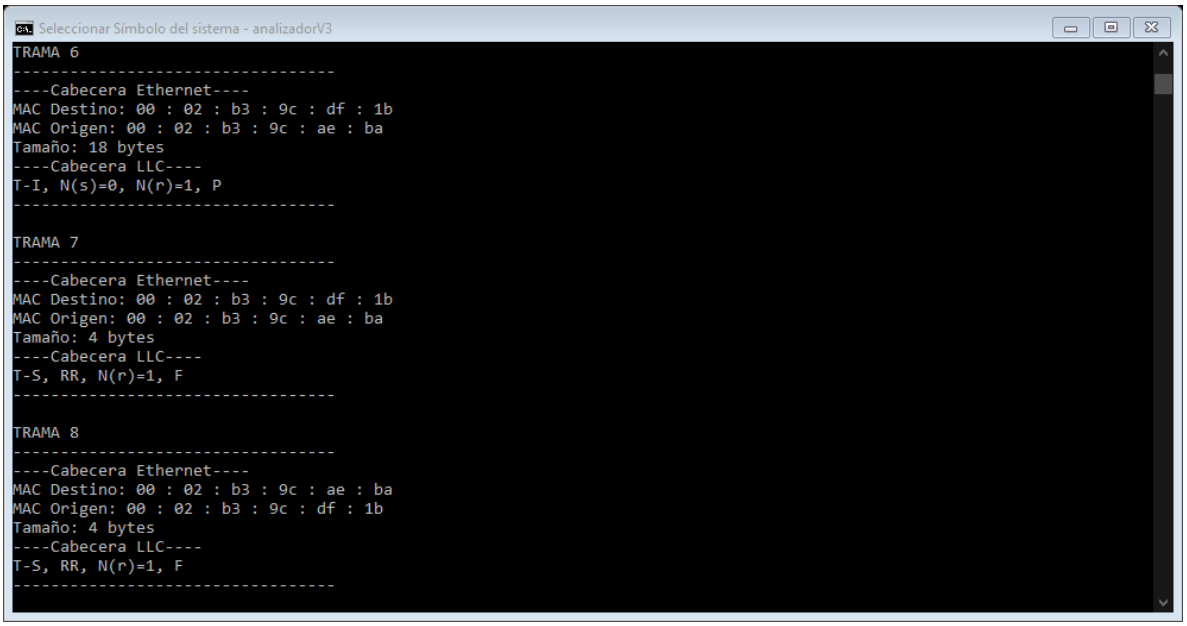
0x02,0xFF,0x53,0xC3,0xE9,0xAB,0x00,0xFF,0x66,0x7F,0xD4,0x3C,0x08,0x00,
0x45,0x02,0x00,0x30,0x2C,0x00,0x40,0x00,0x80,0x06,0x4B,0x74,0xC0,0xA8,
0x01,0x02,0xC0,0xA8, 0x01,0x01,0x04,0x03,0x00,0x15,0x00,0x3B,0xCF,0x44,
0x00,0x00,0x00,0x00,0x70,0x02,0x20,0x00,0x0C,0x34,0x00,0x00,0x02,0x04,
0x05,0xB4,0x01,0x01,0x04,0x02}

};

Capturas del programa






Seleccionar Símbolo del sistema - analizadorV3
TRAMA 6

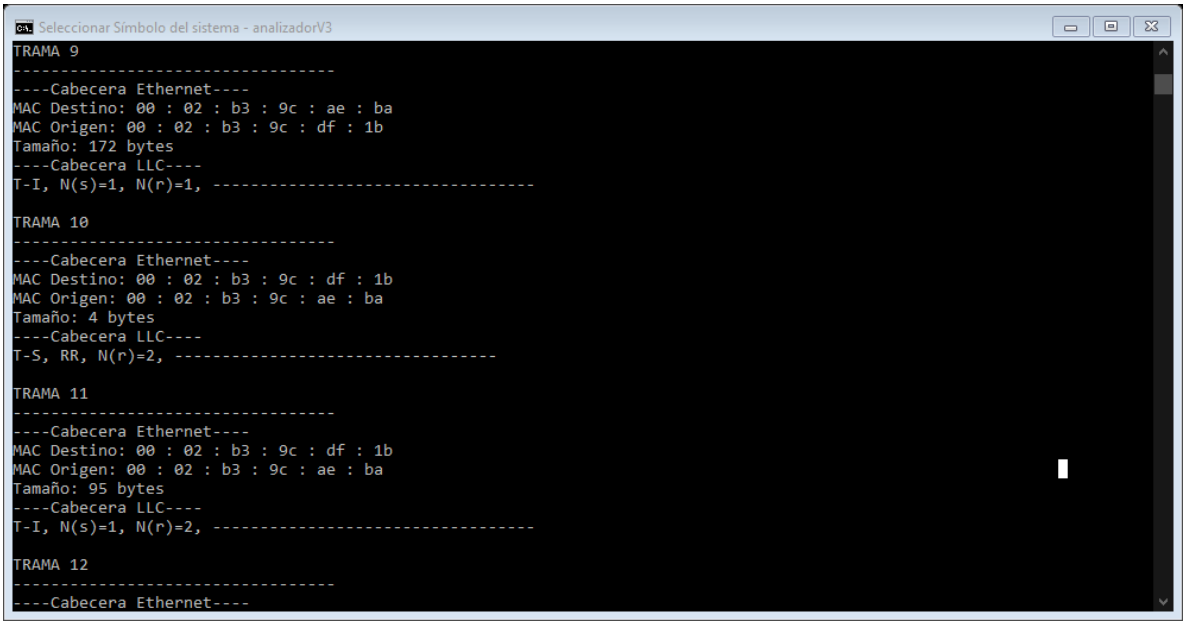
----Cabecera Ethernet----
MAC Destino: 00 : 02 : b3 : 9c : df : 1b
MAC Origen: 00 : 02 : b3 : 9c : ae : ba
Tamaño: 18 bytes
----Cabecera LLC----
T-I, N(s)=0, N(r)=1, P

TRAMA 7

----Cabecera Ethernet----
MAC Destino: 00 : 02 : b3 : 9c : df : 1b
MAC Origen: 00 : 02 : b3 : 9c : ae : ba
Tamaño: 4 bytes
----Cabecera LLC----
T-S, RR, N(r)=1, F

TRAMA 8

----Cabecera Ethernet----
MAC Destino: 00 : 02 : b3 : 9c : ae : ba
MAC Origen: 00 : 02 : b3 : 9c : df : 1b
Tamaño: 4 bytes
----Cabecera LLC----
T-S, RR, N(r)=1, F

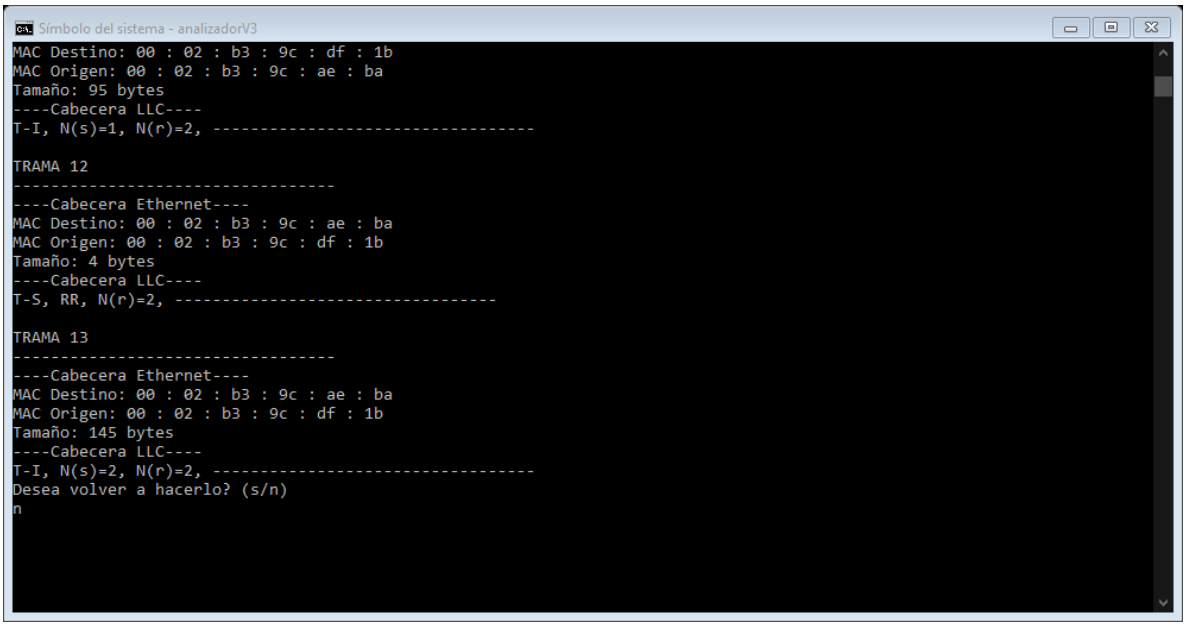

Seleccionar Símbolo del sistema - analizadorV3
TRAMA 9

----Cabecera Ethernet----
MAC Destino: 00 : 02 : b3 : 9c : ae : ba
MAC Origen: 00 : 02 : b3 : 9c : df : 1b
Tamaño: 172 bytes
----Cabecera LLC----
T-I, N(s)=1, N(r)=1, ---
TRAMA 10

----Cabecera Ethernet----
MAC Destino: 00 : 02 : b3 : 9c : df : 1b
MAC Origen: 00 : 02 : b3 : 9c : ae : ba
Tamaño: 4 bytes
----Cabecera LLC----
T-S, RR, N(r)=2, ---
TRAMA 11

----Cabecera Ethernet----
MAC Destino: 00 : 02 : b3 : 9c : df : 1b
MAC Origen: 00 : 02 : b3 : 9c : ae : ba
Tamaño: 95 bytes
----Cabecera LLC----
T-I, N(s)=1, N(r)=2, ---
TRAMA 12

----Cabecera Ethernet----


Símbolo del sistema - analizadorV3
MAC Destino: 00 : 02 : b3 : 9c : df : 1b
MAC Origen: 00 : 02 : b3 : 9c : ae : ba
Tamaño: 95 bytes
----Cabecera LLC----
T-I, N(s)=1, N(r)=2, ----------
TRAMA 12

----Cabecera Ethernet----
MAC Destino: 00 : 02 : b3 : 9c : ae : ba
MAC Origen: 00 : 02 : b3 : 9c : df : 1b
Tamaño: 4 bytes
----Cabecera LLC----
T-S, RR, N(r)=2, ----------
TRAMA 13

----Cabecera Ethernet----
MAC Destino: 00 : 02 : b3 : 9c : ae : ba
MAC Origen: 00 : 02 : b3 : 9c : df : 1b
Tamaño: 145 bytes
----Cabecera LLC----
T-I, N(s)=2, N(r)=2, ----------
Desea volver a hacerlo? (s/n)
n