**Instituto Politécnico Nacional**

Escuela Superior de Cómputo

Reporte Práctica 2

**Integrantes del Equipo:**

Barrera Pérez Carlos Tonatihu

Ramírez Centeno Hugo Enrique

**Grupo:** 2CM11

**Unidad de Aprendizaje:** Redes de Computadoras

**Profesor:** Axel Ernesto Moreno Cervantes

Contenido

[Introducción 2](#_Toc476505312)

[Desarrollo 4](#_Toc476505313)

[Pruebas 4](#_Toc476505314)

[Conclusiones 5](#_Toc476505315)

# Introducción

Una dirección MAC es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet). «MAC» significa Media Access Control, y cada código tiene la intención de ser único para un dispositivo en particular.

Una dirección MAC consiste en seis grupos de dos caracteres, cada uno de ellos separado por dos puntos. 00:1B:44:11:3A:B7 es un ejemplo de dirección MAC.

El objetivo de esta práctica es desarrollar una aplicación en java que permita separar la dirección mac origen, la dirección mac destino y el tipo de trama. De cada paquete ya sea enviado o recibido por la tarjeta de red, además identificar el tipo de trama de acuerdo al RFC 1340.

RFC o (Request for commands) son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos.1 2 Cada RFC constituye un monográfico o memorando que ingenieros o expertos en la materia han hecho llegar al IETF, el consorcio de colaboración técnica más importante en Internet, para que éste sea valorado por el resto de la comunidad. De hecho, la traducción literal de RFC al español es "Petición de comentarios"

En específico el RFC 1340 nos indica los tipos de protocolos, éstos tienen un número asociado el cual va escrito en el encabezado TCP en la parte de protocolo.

PROTOCOL NUMBERS

In the Internet Protocol (IP) [45,105] there is a field, called

Protocol, to identify the the next level protocol. This is an 8 bit

field.

Assigned Internet Protocol Numbers

Decimal Keyword Protocol References

------- ------- -------- ----------

0 Reserved [JBP]

1 ICMP Internet Control Message [97,JBP]

2 IGMP Internet Group Management [43,JBP]

3 GGP Gateway-to-Gateway [60,MB]

4 IP IP in IP (encapsulation) [JBP]

5 ST Stream [49,JWF]

6 TCP Transmission Control [106,JBP]

7 UCL UCL [PK]

8 EGP Exterior Gateway Protocol [123,DLM1]

9 IGP any private interior gateway [JBP]

10 BBN-RCC-MON BBN RCC Monitoring [SGC]

11 NVP-II Network Voice Protocol [22,SC3]

12 PUP PUP [8,XEROX]

13 ARGUS ARGUS [RWS4]

14 EMCON EMCON [BN7]

15 XNET Cross Net Debugger [56,JFH2]

16 CHAOS Chaos [NC3]

17 UDP User Datagram [104,JBP]

18 MUX Multiplexing [23,JBP]

19 DCN-MEAS DCN Measurement Subsystems [DLM1]

20 HMP Host Monitoring [59,RH6]

21 PRM Packet Radio Measurement [ZSU]

22 XNS-IDP XEROX NS IDP [133,XEROX]

23 TRUNK-1 Trunk-1 [BWB6]

24 TRUNK-2 Trunk-2 [BWB6]

25 LEAF-1 Leaf-1 [BWB6]

26 LEAF-2 Leaf-2 [BWB6]

27 RDP Reliable Data Protocol [138,RH6]

28 IRTP Internet Reliable Transaction [79,TXM]

29 ISO-TP4 ISO Transport Protocol Class 4 [63,RC77]

30 NETBLT Bulk Data TransferProtocol [20,DDC1]

31 MFE-NSP MFE Network Services Protocol [124,BCH2]

32 MERIT-INP MERIT Internodal Protocol [HWB]

33 SEP Sequential Exchange Protocol [JC120]

34 3PC Third Party Connect Protocol [SAF3]

35 IDPR Inter-Domain Policy Routing Protocol [MXS1]

36 XTP XTP [GXC]

37 DDP Datagram Delivery Protocol [WXC]

38 IDPR-CMTP IDPR Control Message Transport Proto [MXS1]

39 TP++ TP++ Transport Protocol [DXF]

40 IL IL Transport Protocol [DXP2]

41-60 Unassigned [JBP]

61 any host internal protocol [JBP]

62 CFTP CFTP [50,HCF2]

63 any local network [JBP]

64 SAT-EXPAK SATNET and Backroom EXPAK [SHB]

65 KRYPTOLAN Kryptolan [PXL1]

66 RVD MIT Remote Virtual Disk Protocol [MBG]

67 IPPC Internet Pluribus Packet Core [SHB]

68 any distributed file system [JBP]

69 SAT-MON SATNET Monitoring [SHB]

70 VISA VISA Protocol [GXT1]

71 IPCV Internet Packet Core Utility [SHB]

72 CPNX Computer Protocol Network Executive [DXM2]

73 CPHB Computer Protocol Heart Beat [DXM2]

74 WSN Wang Span Network [VXD]

75 PVP Packet Video Protocol [SC3]

76 BR-SAT-MON Backroom SATNET Monitoring [SHB]

77 SUN-ND SUN ND PROTOCOL-Temporary [WM3]

78 WB-MON WIDEBAND Monitoring [SHB]

79 WB-EXPAK WIDEBAND EXPAK [SHB]

80 ISO-IP ISO Internet Protocol [MTR]

81 VMTP VMTP [DRC3]

82 SECURE-VMTP SECURE-VMTP [DRC3]

83 VINES VINES [BXH]

84 TTP TTP [JXS]

85 NSFNET-IGP NSFNET-IGP [HWB]

86 DGP Dissimilar Gateway Protocol [74,ML109]

87 TCF TCF [GAL5]

88 IGRP IGRP [18,GXS]

89 OSPFIGP OSPFIGP [83,JTM4]

90 Sprite-RPC Sprite RPC Protocol [143,BXW]

91 LARP Locus Address Resolution Protocol [BXH]

92 MTP Multicast Transport Protocol [SXA]

93 AX.25 AX.25 Frames [BK29]

94 IPIP IP-within-IP Encapsulation Protocol [JXI1]

95 MICP Mobile Internetworking Control Pro. [JXI1]

96 AES-SP3-D AES Security Protocol 3-D [HXH]

97 ETHERIP Ethernet-within-IP Encapsulation [RXH1]

98 ENCAP Encapsulation Header [148,RXB3]

99-254 Unassigned [JBP]

255 Reserved [JBP]

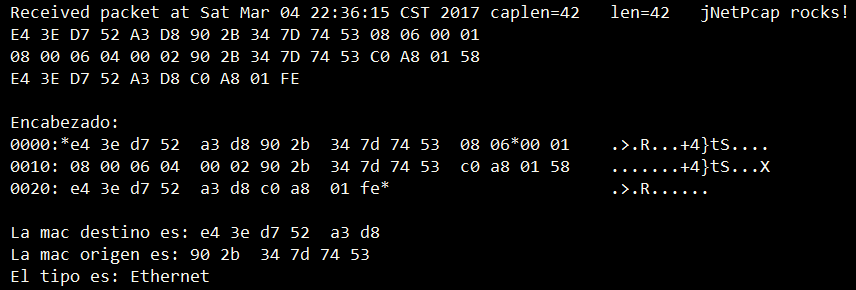
# Desarrollo

Para el desarrollo de la práctica utilizamos una API llamada JnetPcap la cual nos permite capturar paquetes que vayan entrando a la tarjeta de red, asimismo utilizamos una clase en java la cual hacía uso de la API mencionada anteriormente, esta tuvo que ser modificada ya que por defecto arrojaba solo los paquetes capturados, los cambios hechos fueron para poder procesar el encabezado de la capa de enlace de datos del protocolo TCP/IP. Dentro del procesamiento del encabezado se realizó la separación de las direcciones MAC destino, MAC origen y el tipo de trama.

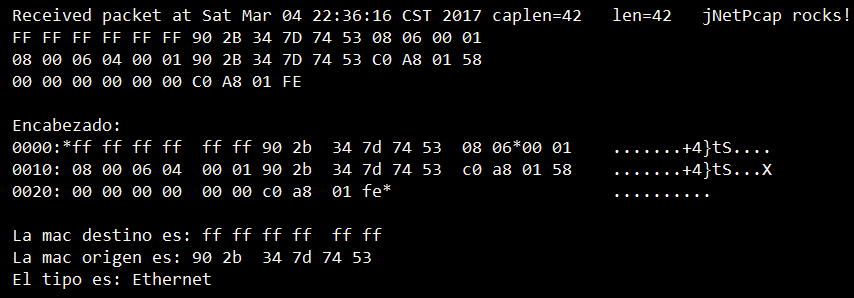
Para identificar el tipo de trama nos basamos en el RFC 1340 el cual nos indica que si el número del protocolo es menor a 1500 es de tipo ethernet.

# Pruebas

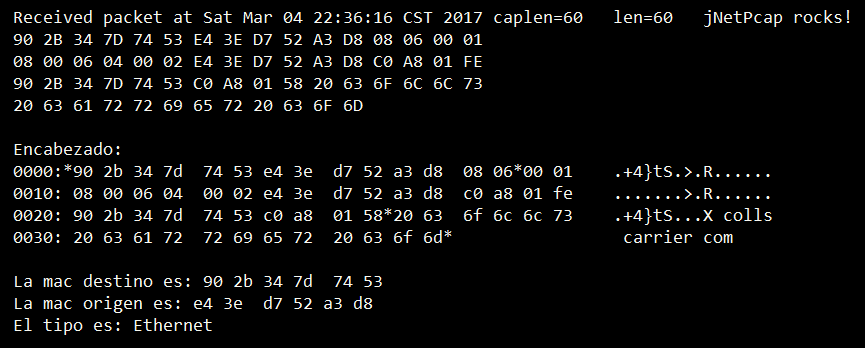
Para las pruebas tomamos capturas de tres paquetes capturados.



Primera trama de datos capturada, se puede observar que la aplicación separa del encabezado la dirección mac destino, la dirección mac origen y el tipo de trama.



Segunda trama de datos capturada; de la misma forma se puede observar la separación de las direcciones mac destino, mac origen y el tipo de trama



Tercera trama de datos capturada.

# Conclusiones

**Tonatihu:** En esta práctica se reforzaron los conocimientos sobre tres componentes de las tramas en concreto la MAC destino, MAC origen y el tipo. Esto se realizó mediante la elaboración de un programa que identifica estos elementos de tramas capturadas, se elaboró con el uso de una librería llamada jnetcap, además de capturar paquetes en tiempo real nos permite trabajar con protocolos y captura del tráfico de red. Y a pesar de que esta es una implementación básica de esta librería en el futuro nos podría ayudar a realizar herramientas como Wireshark.

**Hugo:** Dentro del encabezado de la capa de enlace de datos se encuentran las direcciones mac destino, mac origen y además el tipo de trama, estos conceptos logré aprenderlos mejor con el desarrollo de esta práctica, asimismo reflexioné acerca de estos encabezados y la importancia que tienen hoy en día en las comunicaciones.