Alunos: João F. Carvalho, Jorge C. da Cunha, Matheus J. da Cunha

Professor: Felipe Viel



**Avaliação – Camada de Enlace**

Este relatório tem por finalidade descrever e documentar os processos efetuados para simular a camada de enlace, conforme projetos passados e também responder as perguntas que estão nos roteiros.

**Projeto 1- Wireshark Lab: 802.11**

Este roteiro foi executado baseado no arquivo da documentação Wireshark\_802\_11.pcap que foi aberto no software wireshark e realizado as análises necessários para as questões abaixo.

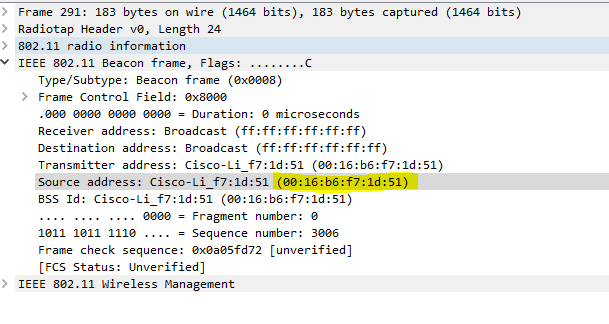
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

R: Os SSID são 30 Munroe ST e Linksys\_SES\_24086

1. What are the intervals of time between the transmissions of the beacon frames the linksys\_ses\_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

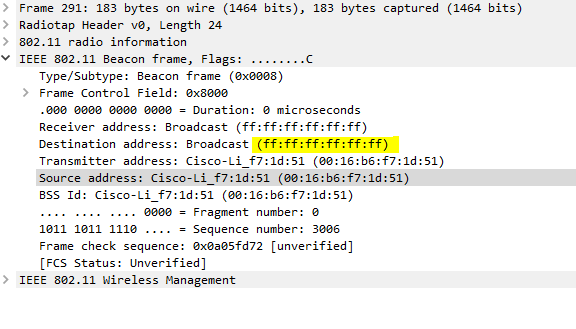
R: O intervalo é 1024 segundos.

1. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from figure 7.13 in the text that the source, destination, and BSS are three adresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).

R: O endereço físico é o 00:16:b6:f7:1d:51

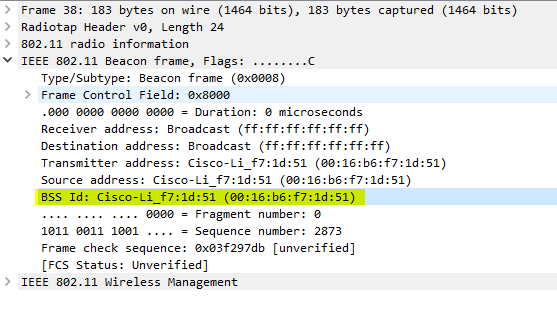
1. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St??

R: O endereço físico de destino é o ff:ff:ff:ff:ff:ff



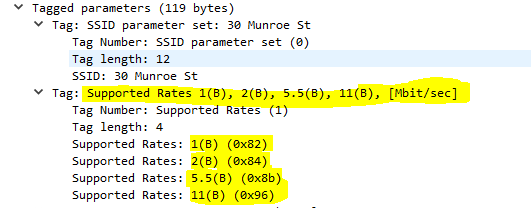
1. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

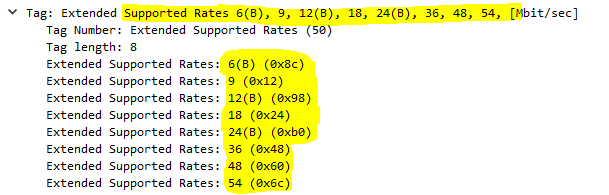
R: O endereço físico BSS é o 00:16:b6:f7:1d:51



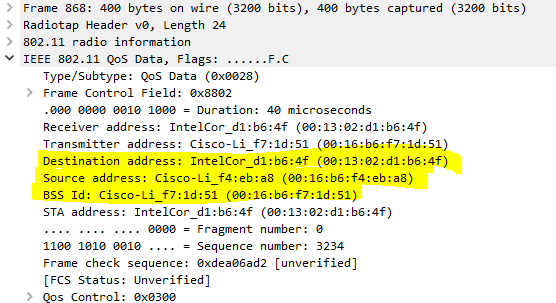
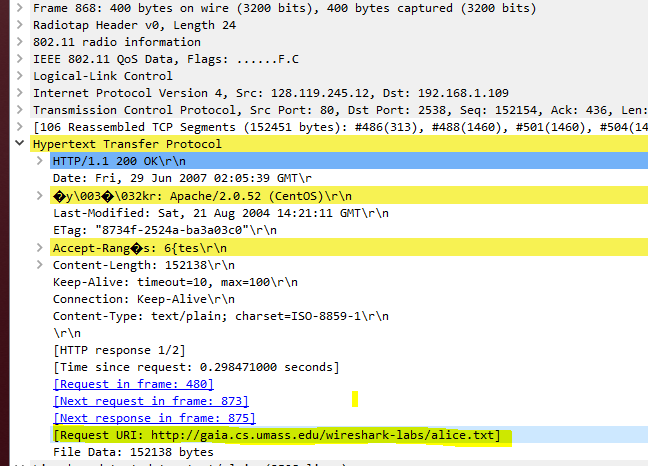
1. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional “extended supported rates. ”What are these rates?

R: As taxas de suporte são: 1.0, 2.0, 5.5,11.0 Mbps. As taxas estendidas são: 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 e 54.0 Mbps





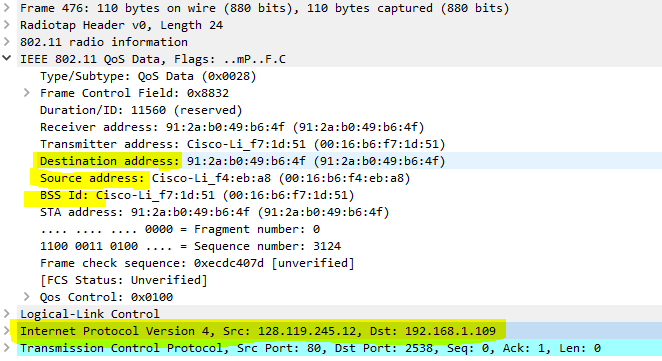
1. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

R: Os endereços MACS presentes em 802.11 são: BSS ID, Source e Destination. O endereço MAC do host wireless é o 00:13:02:d1:b6:4f. O endereço físico do ponto de acesso é o 00:16:b6:f4:eb:a8. Correspondente ao host sem fio que envia este segmento TCP é 00:16:b6:f7:1d:51. O IP correspondente do host sem fio é 192.168.1.109. Do destino o IP é o 128.199.245.12 e este IP corresponde ao host.C:\Users\Jorge\Desktop\802 11\pergunta 7 1.PNG

1. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It’s particularly important that you understand this).

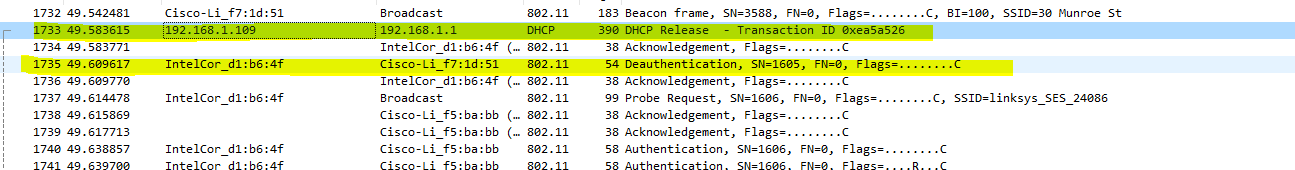
R: BSS id: 00:16:b6:f7:1d:51, Destination: 00:13:02:d1:b6:4f e endereço de origem: 00:16:b6:f4:eb:a8. O MAC corresponde ao host é 00:13:02:d1:b6:4f (destino). Source: 00:16:b6:f4:eb:a8. O endereço MAC do remetente no quadro não corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado dentro deste datagrama, porque o TCP SYNACK O endereço IP é 128:199:245:12, mas o endereço IP de destino é 192.168.1.109.

C:\Users\Jorge\Desktop\802 11\pergunta 8 1.PNG



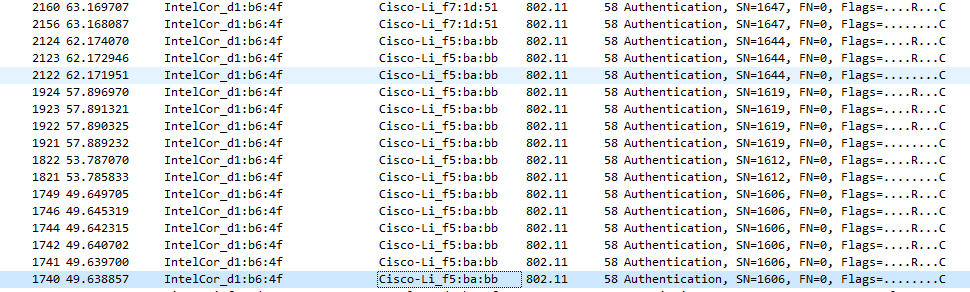
1. What two actions are taken (i.e., frames are sent) by the host in the trace just after t=49, to end the association with the 30 Munroe St AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don’t see here?

R: Um DHCP é enviado para 192.168.1.1. O host envia um quadro DEAUTHENTICATION após 0,02s



1. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys\_ses\_24086 AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around t=49? .

R: São enviadas no total 17 mensagens.



1. Does the host want the authentication to require a key or be open?

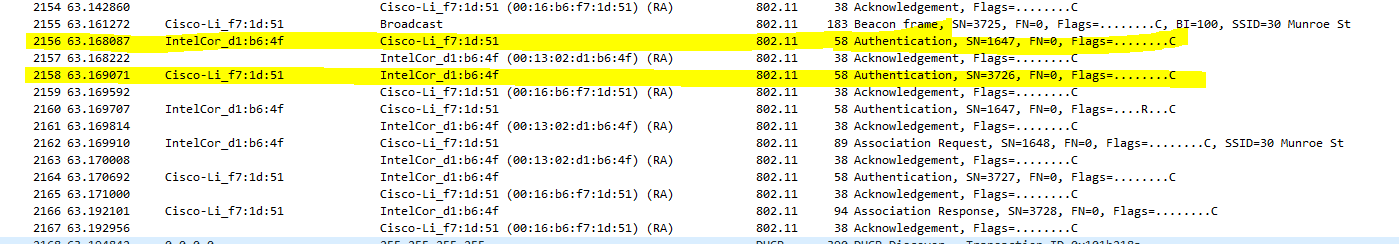
R: Exige uma autenticação

1. Do you see a reply AUTHENTICATION from the linksys\_ses\_24086 AP in the trace?

R: Não possuí retorno.

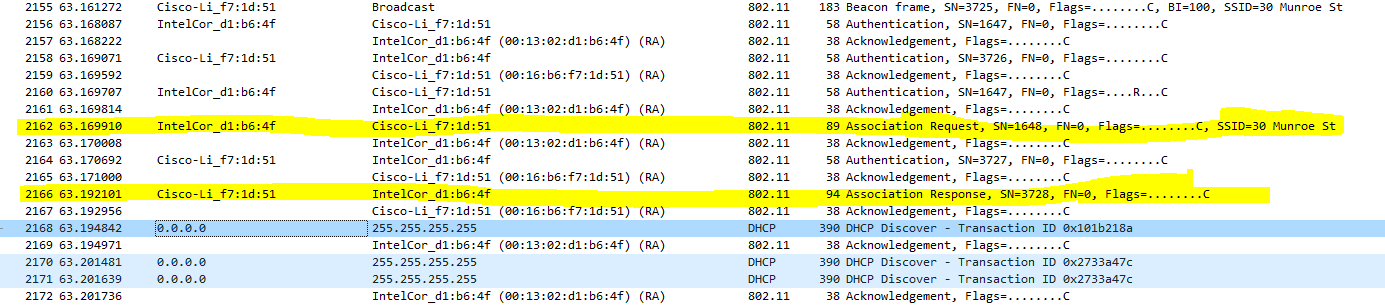
1. Now let’s consider what happens as the host gives up trying to associate with the linksys\_ses\_24086 AP and now tries to associate with the 30 Munroe St AP. Look for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression “wlan.fc.subtype== 11and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f” to display only the AUTHENTICATION frames in this trace for this wireless host.)

R: Há um quadro de AUTENTICAÇÃO de 00:13:02:d1:b6:4f a 00:16:b7:f7:1d:51 quando t = 63.168087. A AUTENTICAÇÃO enviada de volta em t = 63,169071



1. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression “wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f” to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

R: Associate request do host para o SSID 30 Munroe St em t = 63.169910 e respondeu em t 63.192101.



1. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

R: As taxas possíveis são 1, 2, 5,5, 11, 6, 9, 12, 18, 24, 32, 48, 54 Mbps. Basta analisar as taxas "supported" e "exnteded" dos AP em broadcast já respondidas na questão 6.

1. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames? (To answer this last question, you’ll need to dig into the online references cited earlier in this lab).

R: Probe request: Source: 00:12:f0:1f:57:13, destination: ff:ff:ff:ff:ff:ff, BSSID: ff:ff:ff:ff:ff:ff

Probe response: Source: 00:16:b6:f7:1d:51, destination: 00:16:b6:f7:1d:51, BSSID: 00:16:b6:f7:1d:51

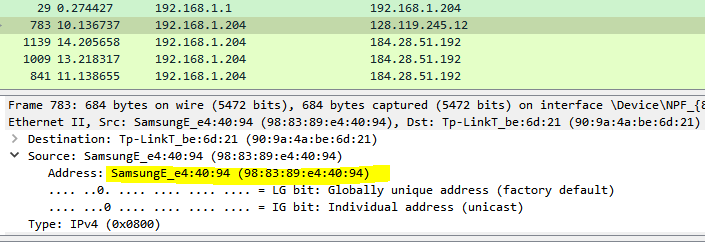
É uma transmissão para procurar um ponto de acesso do host.

**Projeto 1 – Ethernet and ARP**

Este roteiro foi executado em um seguinte cenário: Notebook SAMSUNG utilizando uma rede wireless, onde se conectava ao roteador da TP-LINK que era conectado no modem da NET. Utilizado a URL <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html> para capturar as requisições no wireshark e realizar as seguintes análises para os questionários abaixo.

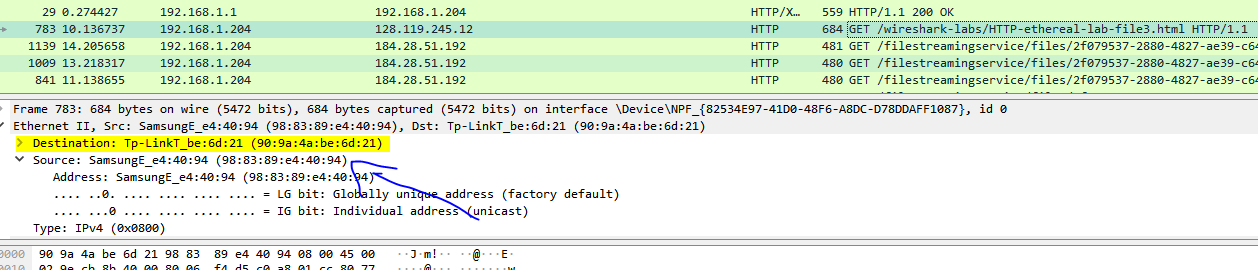
1. What is the 48-bit Ethernet address of your computer?

R: O endereço é o 98:83:89:e4:40:94 (SamsungE\_e4:40:94)



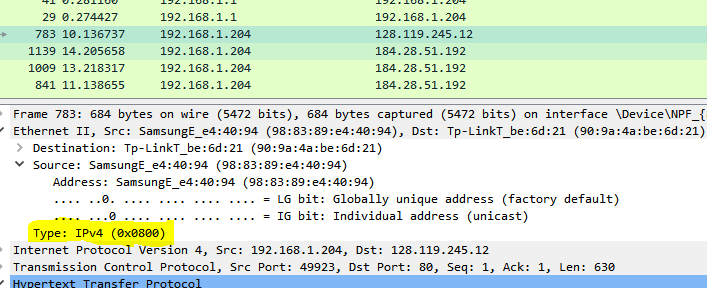
1. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here. ]

R: O endereço é o 90:9a:4a:be:6d:21 (Tp-LinkT\_be:6d:21)



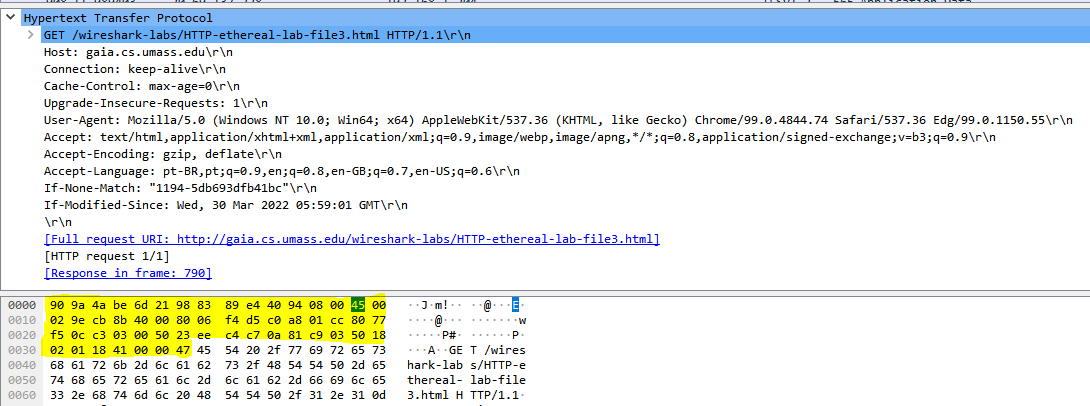
1. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

R: IPv4 (0x0800)



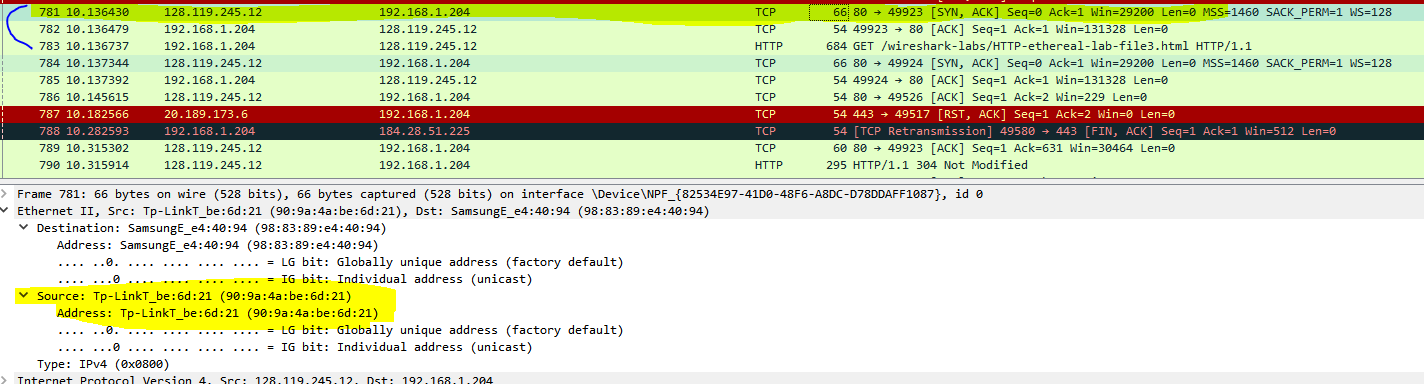
1. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

R: Sua aparição é em 55 bytes.



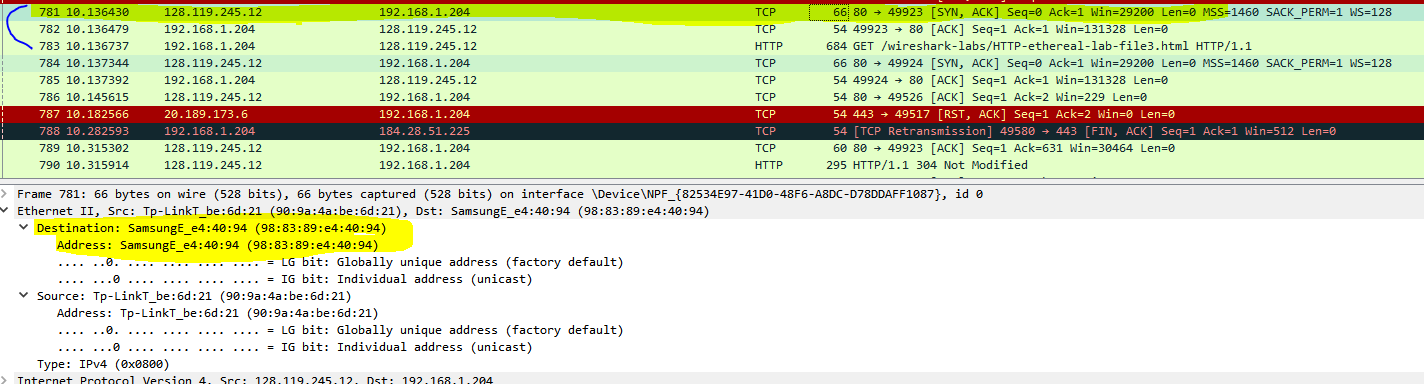
1. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

R: É o de meu roteador Tp-LinkT\_be:6d:21 (90:9a:4a:be:6d:21)



1. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

R: Pertence ao meu computador SamsungE\_e4:40:94 (98:83:89:e4:40:94)

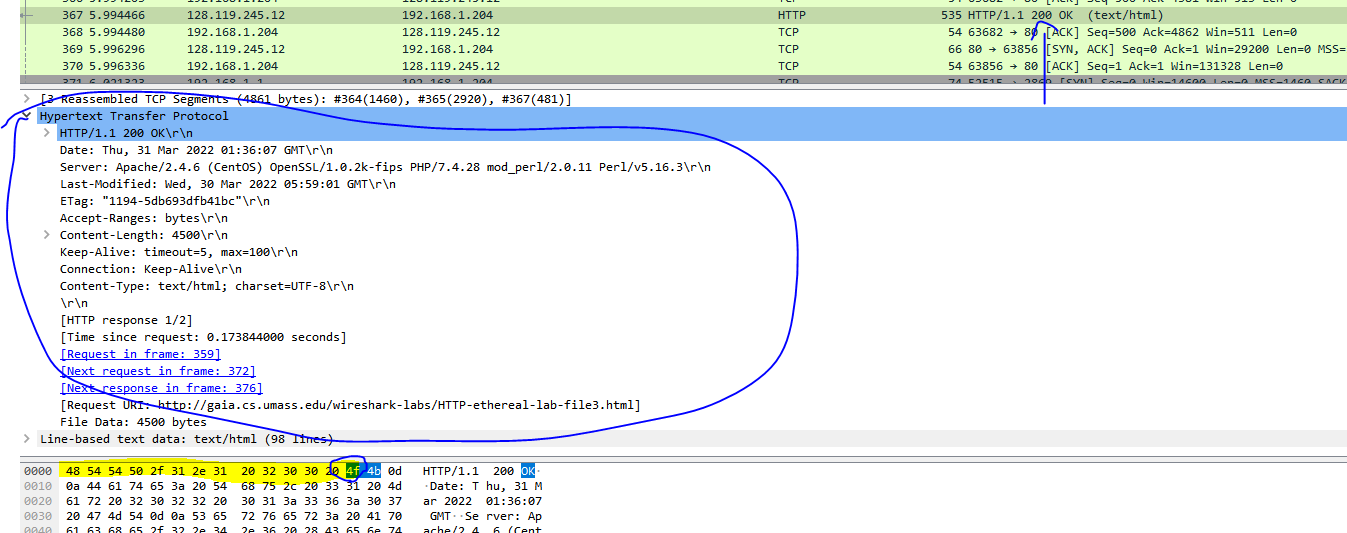


1. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

R: 0x0800 (IPv4)

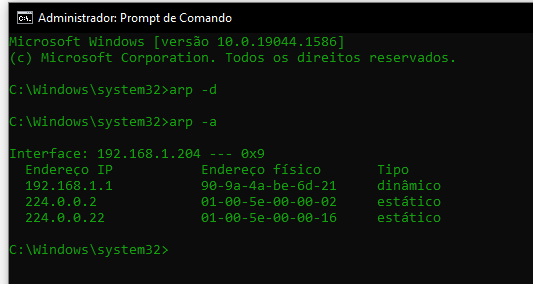
1. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

R: Sua aparição é em 14 bytes



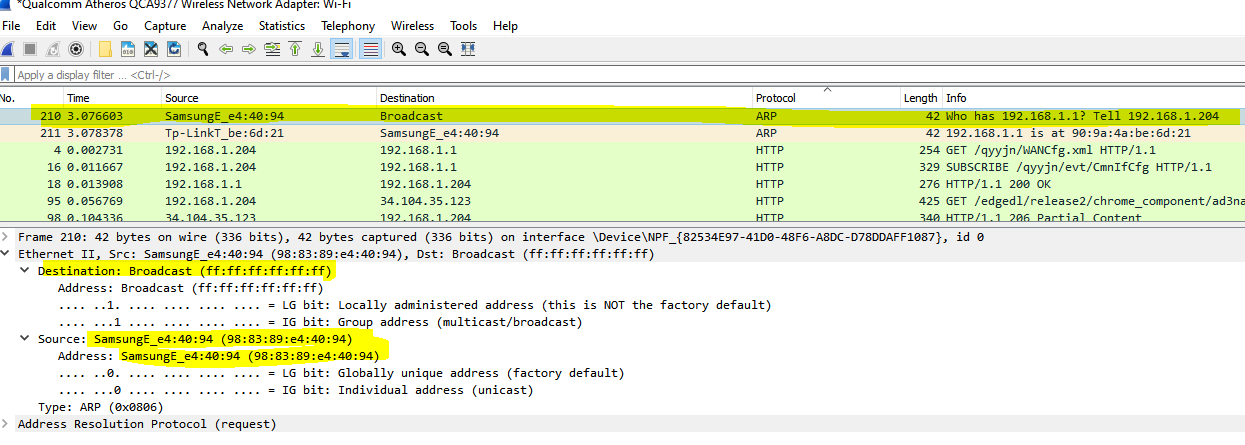
1. Write down the contents of your computer’s ARP cache. What is the meaning of each column value?

R: Representam o endereço IP na camada de rede, o endereço MAC para se comunicar fisicamente com o hardware que está localizado nesse endereço IP e se ele está mudando ou não (dinâmico) ou estático.



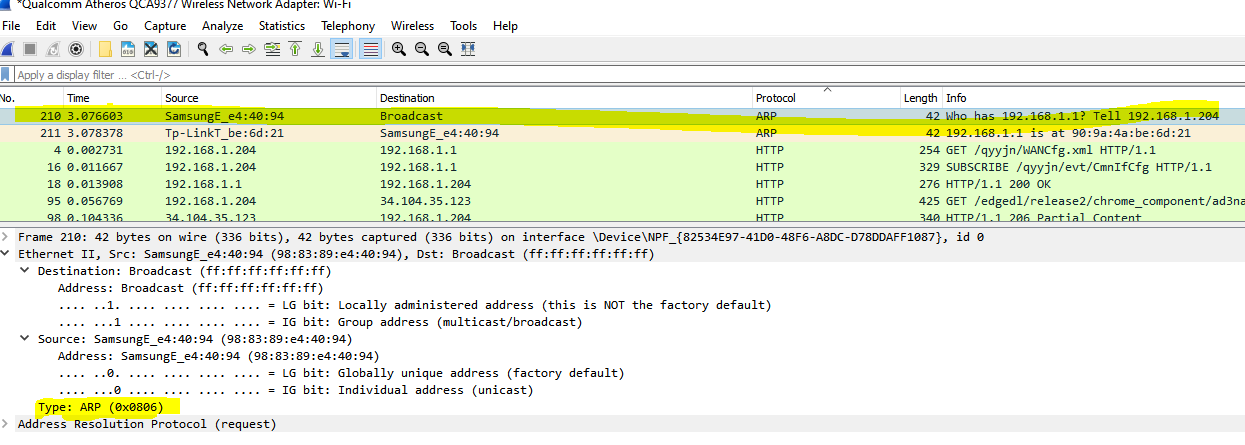
1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

R: O endereço origem é o 98:83:89:e4:40:94 e o destino é o ff:ff:ff:ff:ff:ff.



1. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

R: ARP (0x0806)



1. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.
2. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

R: 21 bytes

1. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

R: 001

1. Does the ARP message contain the IP address of the sender?

R: Sim

1. Now find the ARP reply that was sent in response to the ARP request.
2. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

R: 21 bytes

1. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

R: 002

1. Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the ethernet address whose corresponding IP address is being queried?

R: No endereço MAC do remetente

1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

R: Origem: 98:83:89:e4:40:94. Destino: ff:ff:ff:ff:ff:ff

**Projeto 2 - Simulação Packet Tracer**