# <u>TP n° 03</u>

# Analyse du protocoleEthernet sousWireshark

## 1. Objectif

L'objectif de ce TP est l'étude du fonctionnement du protocole Ethernet via l'analyse du trafic en utilisant Wireshark.

## 2. Encapsulation dans la pile TCP/IP

Par exemple pour un message HTTP l'ordre d'encapsulation est « HTTP-TCP-IP-Ethernet ». Noter que pour Wireshark, il sera affiché inversement « Ethernet-IP-TCP-HTTP ».



La figure suivante illustre la structure d'une trame capturée :



La trame Ethernet contient l' « Entête Ethernet » et le champ « Données Ethernet ». Ce dernier contient le paquet IP dont la structure n'est pas reconnue par la couche Ethernet, et ainsi c'est à la couche supérieure de déterminer son en-tête et ses données. De même pour le champ Données IP qui contient le message TCP, et ainsi de suite. La figure suivante illustre la structure (ainsi que la succession des entêtes des différents protocoles encapsulés) pour un message http capturé.



La taille des en-têtes d'un paquet peut être calculée en sachant sa structure (les différents champs qui les constituent). Par exemple, l'entête Ethernet est de 14 octets, l'entête IP et TCP sont de 20 octets chacun. Noter que la taille de l'entête peut être variable, qui est le cas de l'entête HTTP.

Wireshark affiche aussi, tout en bas dans la barre d'état, la taille d'entête du protocole sélectionné dans la zone (2). Dans la figure précédente, la barre d'état indique que la taille de l'entête Ethernet est de 14 octets.

### 3. Protocole Ethernet

Voici la structure de la trame Ethernet :



Soit un trafic réseau capturé à l'aide de Wireshark. Sélectionner un paquet dans la zone (1), et dans la zone (2) appuyer sur [+] du niveau Ethernet pour voir les différents champs d'en-tête Ethernet.

*Module : Réseaux* 2<sup>ème</sup> Année Informatique C.U. Abdelhafid Boussouf - Mila Année universitaire : 2023/2024 Destination Protocol Length Info Time Source 192.168.43.135 88 9.426696 193.194.69.133 569 GET / HTTP/1.1 нттр 120 9 624706 193, 194, 69, 133 192, 168, 43, 135 HTTP 1041 HTTP/1.1 200 OK (text/html) 524 GET /theme/yui\_combo.php?3.17.2/cssbutton/css 646 GET /course/index.php?categoryid=8 HTTP/1.1 232 23, 258511 192,168,43,135 193, 194, 69, 133 HTTP 235 23.310647 192.168.43.135 193.194.69.133 нттр 240 24.087262 192.168.43.135 281 HTTP/1.1 200 OK 193.194.69.133 нттр (text/css) 242 24.110712 192.168.43.135 193.194.69.133 HTTP 1039 GET /theme/yui\_combo.php?m/1677996001/core/wid 250 24.268023 193, 194, 69, 133 192.168.43.135 HTTP 862 HTTP/1.1 200 OK (application/javascript) 353 30.029695 192.168.43.135 193.194.69.133 676 GET /course/index.php?categoryid=17 HTTP/1.1 HTTP 604 HTTP/1.1 200 OK (text/html) 373 30.956267 193, 194, 69, 133 192.168.43.135 нттр 416 35.659859 192,168,43,135 193, 194, 69, 133 нттр 677 GET /course/index.php?categoryid=19 HTTP/1.1 420 35.938237 192.168.43.135 193.194.69.133 HTTP 677 GET /course/index.php?categoryid=19 HTTP/1.1 442 36,633396 193,194,69,133 192,168,43,135 HTTP 540 HTTP/1.1 200 OK (text/html) ⊕ Frame 88: 569 bytes on wire (4552 bits), 569 bytes captured (4552 bits) on interface 0 🗏 Et ⊞ Internet Protocol Version 4, Src: 192.168.43.135, Dst: 193.194.69.133 ⊕ Transmission Control Protocol, Src Port: 51216, Dst Port: 80, Seq: 1, Ack: 1, Len: 515 Hypertext Transfer Protocol 0000 0010 0020 0030 
 46
 8c
 1f
 6c
 4a
 bf
 14
 2d

 02
 2b
 14
 e0
 40
 00
 80
 06

 45
 85
 c8
 10
 00
 50
 40
 1b

 00
 40
 9c
 7e
 00
 00
 47
 45

 2f
 31
 2e
 31
 0d
 0a
 48
 67

 72
 6e
 69
 6e
 72
 2e
 36
 55

 76
 2d
 6d
 69
 6c
 61
 2e
 64

 63
 74
 69
 6f
 6e
 3a
 20
 6b

 65
 0d
 0a
 55
 70
 67
 72
 61

 75
 72
 65
 2d
 52
 65
 71
 75

 0a
 55
 73
 65
 72
 2d
 41
 67
.+..@....... E....P@...4y92.P. .@.~..GE T / HTTP /1.1..Ho st: elea rning.ce ntre-uni v-mila.d z..Conne ction: k eep-aliv +..@ 0040 0050 0060 0070 eep-aliv de-Insec ests: 1. 0070 0080 0090 00a0 e..Upgra de-Insec ure-Requ ests: 1. .User-Ag ent: Moz Ethernet (eth), 14 bytes Packets: 734 · Displayed: 25 (3,4%) · Dropped: 0 (0,0%)

Noter que :

 $\Box$  Le champ « Préambule » ne figure pas dans la trame car il ne contient pas de données utiles, et il est seulement un mécanisme pour aider la carte réseau à identifier le début de la trame.

 $\Box$  Il y a une adresse de destination et une adresse source. Wireshark déchiffre les 3 premiers octets de l'adresse et nous indique le fabricant de la carte. Par exemple Huawei.

□ Les trames Ethernet sont généralement de type "Ethernet II". Ceci est connu grâce au champ « Type ».

Noter que dans le cas d'une trame Ethernet I (IEEE 802.3), il y a le champ « Longueur » au lieu de « Type », et qui indique la longueur de la trame Ethernet.

 $\Box$  Le champ « Type » contient une valeur hexadécimale qui indique le protocole de la couche supérieure concerné par la trame. Par exemple, si sa valeur est 0x0800 donc la trame est destinée au protocole IP, et ainsi le champ « Données » de la trame Ethernet contient le paquet IP.

 $\Box$  Le champ « Données » commence par l'en-tête du protocole de la couche Internet (dans le cas de la figure, c'est l'entête du paquet IP).

 $\Box$  Le champ « Données » peut contenir des données de remplissage dans le cas d'une trame de taille inférieure à 64 octets.

□ Il n'y a pas de champ CRC. Il existe mais il est invisible pour le système ou pour Wireshark, car il est directement utilisé (consommé) par l'équipement (niveau Ethernet) qui envoi et/ou reçoit les trames où il calcule la somme de contrôle et vérifie la présence d'erreurs.

## 4. Le protocole ARP

ARP est utilisé pour trouver l'adresse Ethernet (l'@ MAC) correspondante à une adresse IP locale. Les combinaisons [@IP - @MAC] sont sauvegardées dans une mémoire cache qui peut être manipulée en utilisant des commandes comme suit :

1. Consulter le cache ARP : Taper la commande « arp -a » dans l'invite de commande.

C:\Windows\system32\cmd.exe	a man because Tasks	
Microsoft Windows Evers: Copyright (c) 2009 Micro	ion 6.1.7601] psoft Corporation. Tous	s droits réservés.
C:\Users\Meriem.MERIEM-]	PC>arp -a	
Interface : 192.168.43.2 Adresse Internet 192.168.43.1 192.168.43.255 224.0.0.22 224.0.0.251 224.0.0.252 239.255.255.250 255.255.255.255	232 0xc Adresse physique 46-8c-1f-6c-4a-bf 14-2d-27-78-de-bb ff-ff-ff-ff-ff-ff 01-00-5e-00-00-fb 01-00-5e-00-00-fb 01-00-5e-07-ff-fa 01-00-5e-7f-ff-ff	Type dynamique dynamique statique statique statique statique statique statique statique
Interface : 192.168.56. Adresse Internet 192.168.56.255 224.0.0.22 224.0.0.251 224.0.0.252 239.255.255.250	1 0x12 Adresse physique ff-ff-ff-ff-ff-ff 01-00-5e-00-00-16 01-00-5e-00-00-fb 01-00-5e-00-00-fc 01-00-5e-7f-ff-fa	Type statique statique statique statique statique
C:\Users\Meriem.MERIEM-1	PC>_	

2. Supprimer une entrée dans le cache ARP : Lancer l'invite de commande cette fois-ci en cliquant avec le bouton droit et en choisissant " exécuter en tant qu'administrateur ". Ensuite, taper la commande : « arp –d @IP »

Par exemple, pour effacer l'@IP 192.168.1.1 de la cache ARP, on tape : arp -d 192.168.1.1

#### 4.1. Capture d'un trafic ARP

Dans la salle de TP, la connexion d'un ordinateur au réseau internet se fait selon le schéma dans la figure suivante :



Toute requête lancée par l'ordinateur passe par la passerelle. Ceci est aussi le schéma de connexion de l'ordinateur de la maison connecté à Internet à travers un modem. Dans ce cas, ce modem est la passerelle. Rappeler que la passerelle est l'équipement (généralement un routeur) local que la machine utilise pour se connecter au réseau internet.

C:\Windows\system32\c	md.exe			
C:\Users\Meriem.MER	IEM-PC>netstat -r			
Liste d 2400 ff 1448 5a b6 38 6 1248 5a b6 38 6 11a0 1d 48 d1 3 1808 00 27 00 8 100 00 00 00 00 1300 00 00 00 00 1900 00 00 00 00	51 2a 72 8c 8 75Realte 7 a7Realte 4 8cVirtua Softwa 10 00 00 e0 Carte 10 00 00 e0 Teredo 00 00 00 e0 Carte	.Kaspersky Securi oft Uirtual WiFi k RTL&188EE 802.1 k PCIe FE Family 1Box Host-Only Et re Loopback Inter Microsoft ISATAP Tunneling Pseudo Microsoft ISATAP	ty Data Escort Ad Miniport Adapter 1bgn Wi-Fi Adapter Controller hernet Adapter face 1 —Interface #3	lapter er
IPv4 Table de routa	.ge			=====
	-		=======================================	
Destination réseau 0.0.0.0	Masque réseau 0.0.0.0	Adr. passerelle 192.168.43.1	Adr. interface 192.168.43.232	Métrique 25
127.0.0.1 127.0.0.1 127.255.255.255	255.0.0.0 255.255.255.255 255.255.255.255	On-link On-link On-link	127.0.0.1 127.0.0.1 127.0.0.1	306 306 306
192.168.43.0 192.168.43.232	255.255.255.0 255.255.255.255	On-link On-link	192.168.43.232 192.168.43.232	281 281

En utilisant le navigateur web pour charger une page web (ex. la page Google), pour que la requête puisse être envoyée au serveur, l'ordinateur doit connaitre l'@MAC de la passerelle, et ainsi il va utiliser le protocole ARP pour la trouver. L'échange de paquets ARP capturé par Wireshark a donné ceci :

<b>_</b> *	Conne	xion ré	seau sa	ns fil [\	Nires	hark 2	2.3 (	v2.2.3	-0-g57	531c	:d)]		-						C		٦.								A		x
<u>F</u> ile	<u>E</u> dit	View	<u>G</u> o	<u>C</u> aptu	ire	<u>A</u> nalyz	e S	atisti	cs Te	eleph	ony	<u>T</u> ools	Inter	nals	<u>H</u> elp																
0	•		ø			<b>X</b> 6	2	Q	<b>(</b> )	¢	» T	⊉		F	Ð	0.0	Q 🗹	ĺ	<b>¥</b> [	2 🕫	} %										
Filte	er: arj	þ											-	Expres	sion	Clear	Apply	/ Sa	ave												
No.		Time		🔺 Sc	ource					De	stinati	on			P	otocol	Leng	gth	Info	0											
	1853	11.6	7052	7 4	6:8	::1f:	6c:	4a:b	f	Ho	onHai	Pr_3	8:68	:75	A	RP		42	2 Wh	o has	s 19	2.168	3.43	. 232	?т	[e]]	19	2.168	8.43	.1	
	1854	11.6	7055	2 Н	onHa	aiPr_	38:	68:7	5	46	6:8c:	1f:6	ic:4a	:bf	A	RP		42	2 1 9	2.168	8.43	.232	is	at 4	8:5	ia:b	6:3	8:68:	:75		
	5532	39.0	6225	0 4	6:8	::1f:	6c:	4a:b	f	Ho	onHai	Pr_3	8:68	:75	A	RP		42	2 Wh	o has	s 19	2.168	3.43	. 232	?т	re11	19	2.168	8.43	.1	
	5533	39.0	6228	4 н	onHa	aiPr_	.38:	68:7	5	46	5:8c:	1f:0	ic:4a	:bf	A	RP		42	2 1 9	2.168	8.43	.232	is	at 4	8:5	ia:b	6:3	8:68:	:75		
•													11																		۰.
E F	rame	1853	: 42	bvte	s o	n wir	e (	(336	bits	5).	42 b	vtes	capt	tured	(33	5 bit	s) or	n ir	nter	face	0										
ΞE	ther	net I	I, S	rc: 4	6:8	c:1f	: 6c :	:4a:1	of (4	6:8	c:1f	:6c:	4a:bf	F), [	st:	HonHa	iPr_3	38:6	68:7	5 (4	8:5a	:b6:	38:6	8:75	6)						
	ddre	ss Re	solu	tion	Pro	toco	(r	eque	est)																						
	Har	dware	typ	e: Et	her	net (	(1)																								
	Pro	tocol	typ	e: IP	'v4	(0x08	300)	)																							
	Har	dware	siz	e: 6																											
	Pro	tocol	siz	e: 4																											
	орс	ode:	requ	est (	1)																										
	Sen	der M	AC a	ddres	s:	46:80	::1f	:6C	:4a:b	of (	46:8	c:1f	:6c:4	la:bf	•)																
	Sen	der I	P ad	dress	: 1	92.16	8.4	13.1																							
	Tar	get M	AC a	ddres	s:	00:00	):00	)_00:	.00:0	00 (	00:00	0:00	:00:0	00:00	))																
	Tar	get I	P ad	dress	: 1	92.10	j <b>8.</b> 4	13.23	32																						
000	0 4	8 5a	b6 3/	3 68	75	46 80	- 1	f 60	4a	bf	08.0	5 00	01	HZ.	8huF	11															
001	ŏ Ö	8 00	06 04	4 00	01 4	46 80	1	f 60	: 4a	bf	c0 a	3 2b	01		F	. 15	+.														
002	0 0	0 00	00 00	00 (	00	c0 a8	2	2b e8								+.															
	Ad	dress Re	esolutio	on Prot	ocol	(arp), 2	8 byt	tes	Pack	kets: 7	7336 • 1	)ispla.	Pro	ofile: D	efault																

Noter qu'un filtre est appliqué pour n'afficher que les paquets ARP.

Il existe deux types de paquets ARP (distingués par la colonne Info de la zone 1) :

1. Paquet Demande : La ligne Info de ce paquet contient « Who has 192.168.43.232? ... » (Voir la trame n° 1853).

2. Paquet Réponse : La ligne Info de ce paquet contient « @IP is at @MAC », voir la trame n° 1854.

En sélectionnant la trame n°1853 et cliquant sur [+] de « Adresse Resolution Protocol » dans la zone (2). Les champs suivants s'affichent :

- « Hardware Type » et « Protocol Type » : qui indiquent que la carte réseau dont on cherche son @ physique est une carte Ethernet, et on dispose de son adresse logique qui est une @IP.
- « Hardware size » et « Protocol size » : définissent la taille de l'@ physique (matériel) et celle logique (protocole) sur 6 octets et 4 octets, respectivement.
- « Opcode » : contient la valeur request (1) qui indique qu'il s'agit d'une requête.
- « Sender MAC » « Sender IP » « Target MAC » et « Target IP » : définissent, respectivement, l'@ MAC (Ethernet) et IP de l'émetteur, et l'@ MAC et IP du destinataire.

En sélectionnant la trame n° 1854 et cliquant sur [+] de « Adresse Resolution Protocol », les champs qui changent de valeurs par rapport à la trame précédente sont :

- « Opcode » où il contient la valeur reply (2) qui veut dire que c'est une trame de réponse.
- « Sender MAC » « Sender IP » « Target MAC » et « Target IP » : où leurs valeurs sont inversées (Sender devient Target et Target devient Sender) puisque le destinataire devient lui l'émetteur.

Address Resolution Protocol (reply)	
Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	10 1140
Hardware size: 6	Lemac
Protocol size: 4	recherche
Opcode: reply (2)	·
Sender MAC address: HonHaiPr_38:68:75	(48:5a:b6:38:68:75)
Sender IP address: 192.168.43.232	
Target MAC address: 46:8c:1f:6c:4a:bf	(46:8c:1f:6c:4a:bf)
Target IP address: 192.168.43.1	
-	

## 5. Travail demandé

I. Capturez un trafic réseau comme suit : lancez une capture Wireshark, ensuite chargez une page web (ex. entrez dans le site : elearning.centre-univ-mila.dz et consultez des cours) via votre navigateur. Arrêtez la capture après un moment.

1. Donnez le n° d'un paquet contenant un message GET de HTTP.

2. Quelle est l'adresse MAC de destination dans ce paquet ? Est-ce l'adresse Ethernet de votre ordinateur ? Expliquez.

3. Donnez le n° d'un paquet contenant un message OK de HTTP.

4. Quelle est l'adresse MAC source dans ce paquet ? Est-ce l'adresse Ethernet du serveur web hébergeant la page web demandée ? Expliquez.

5. Quelle est l'adresse de broadcast Ethernet ? Donnez le numéro d'une trame de diffusion Ethernet.

6. Quel champ dans l'en-tête Ethernet permettant de déterminer à quel protocole de la couche supérieure la trame est destinée ?

7. Donnez un exemple (n° du paquet capturé) d'un paquet destiné au protocole IP. Quelle est la valeur du champ précédent dans ce cas ?

8. Pour un paquet HTTP combien d'octets pour chacune des entêtes : Ethernet, IP et TCP ?

II. Dans cette partie, on essaie de faire en sorte que la machine utilise le protocole ARP pour découvrir l'adresse MAC du routeur local (la passerelle). Ensuite on analyse le trafic capturé.

1. Quelle est l'adresse IP de la passerelle ?

2. L'@IP de la passerelle existe-elle dans le cash ARP ?

3. Effacez l'@IP de la passerelle du cache ARP.

4. Lancez une capture en utilisant Wireshark, et utilisez le navigateur web pour charger une page web. Une fois le trafic ARP est capturé, arrêtez la capture.

5. Filtrez les paquets capturés pour n'afficher que les paquets ARP.

6. Donnez le n° d'un paquet ARP demande.

7. Quel est le n° de son paquet ARP réponse ?

8. Quelle est la valeur du champ « Opcode » pour chacun des deux paquets ?

9. Quelle est la taille de l'en-tête ARP pour une demande ? Qu'en est-il d'une réponse ?

10. Quelle est l'adresse MAC cible pour le paquet ARP demande ?

11. Complétez le schéma suivant par les informations des deux paquets ARP :

### Requête ou Réponse

