Capture, Filtrage et Analyse de trames ETHERNET avec le logiciel Wireshark

Wireshark est un programme informatique libre de droit, qui permet de capturer et d'analyser les trames d'information qui transitent par les interfaces de communication du terminal sur lequel il s'exécute. *Wireshark* est ainsi apparenté aux logiciels appelés « Sniffer » ou « analyseur de trafic ». Il est multi-OS et téléchargeable sur le site <u>www.wireshark.com</u>.

Avec *Wireshark*, il est possible de capturer des trames Ethernet en temps réel directement sur les Cartes de communication du terminal, de sauvegarder les résultats de cette capture dans des fichiers qui peuvent être analysés ultérieurement hors ligne. *Wireshark* supporte un très grand nombre de protocoles de communication et de formats de fichiers de capture : Ethernet, ARP, IP, TCP/UDP, HDLC, etc ... libpcap/tcpdump, Sun's snoop/atmsnoop, LanAlyzer, MS Network Monitor, HPUX nettl, AIX iptrace, Cisco Secure IDS, etc....

Durant ce TP, nous allons :

- 1. lancer le programme Wireshark,
- 2. capturer et analyser une trame Ethernet
- 3. définir des filtres pour la capture et la visualisation des trames
- 4. Enregistrer le résultat de cette capture dans un fichier

Etape 1 : Lancement des machines virtuelles VMWARE et de Wireshark

1.1 – Démarrer la machine virtuelle vmware sur votre poste au moyen de la commande suivante :

[user1@machine] \$ vmware&

si nécessaire ajouter le chemin aux répertoires etc/sbin et /bin à la variable d'environnement PATH, en tapant la commande suivante :

[user1@machine] \$ export PATH= "\$PATH":/etc/sbin :/sbin

Lancer la machine virtuelle Serveur (FC5-ServerG) en sélectionnant la machine dans la liste (menu de gauche)

Connectez vous en tant qu'administrateur sur le serveur avec :

login = root mot de passe = etu&reseaux

Lancer la machine virtuelle Cliente (FC5-client) en sélectionnant la machine dans la liste (menu de gauche)

Connectez vous en tant qu'administrateur sur le client avec :

```
login = root
mot de passe = etu&reseaux
```

1.2 Démarrez ensuite l'application *Wireshark*. Créez un raccourci sur votre bureau il vous sera bien utile. Voila comment le sniffer se présente.

UFR de Mathématiques et Informatique

		° 2 9 4	🕸 🕸	주 ⊉ 🔲	• •		
Filter:			Expression.	. Clear Apply		.	
No Time	Source	Destination	Protocol	Info	^		
1 0.00000	0 193.48.200.120	193.48.200.255	NBNS	Name query NB	SERVUFR	•	
2 0.59994	0 193.51.224.14	193.48.200.163	TCP	http > 1872 [s	SYN, ACK		
3 0.64824	8 193.48.200.18	102 48 200 255	COPS	hpp://mars.mat	SEDUCED	•	
5 0 78252	2 193.48.200.120	193 48 200 163	TCP	http > 1872 [9	SERVOFRA		
6 0.82022	3 Cisco fc:3a:bb	Spanning_tree_(f	or STP	Conf. Root = 2	48/00 dc		
7 1.30514	7 Dell_75:be:1c	Broadcast	ARP	who has 193.48	3.200.141	. :	_
8 1.41342	3 193.48.200.198	193.51.224.23	TCP	3121 > http [9	SYN] Seq:		F
9 1.41412	7 193.51.224.23	193.48.200.198	TCP	http > 3121 [s	SYN, ACK	•	
10 1.41417	6 193.48.200.198	193.51.224.23	TCP	3121 > http [/	ACK] Seq=		
11 1.41439	1 193.48.200.198	193.51.224.23	HTTP	GET /1/?BHwnac	l]5I†×3mF		
12 1.41506	6 193.51.224.23	193.48.200.198	TCP	nttp > 3121 [A	ACK] Seq=	1 :	
13 1.62064	0 193.31.224.23	193.48.200.198	HITE	HIP/1.1 200 C	ik (app)	-	
		1 4 2 51 7 7 7 7 2	TCO	21 21 5 6776 10	TIM OCK		
15 1,62205	2 193.51.224.23	193.51.224.23	TCP	3121 > nttp []	IN, ACK		
15 1.62205	1 195.48.200.198 2 193.51.224.23 6 193.48 200 198	193.51.224.23 193.48.200.198 193.51 224 23	TCP TCP TCP	3121 > http [F http > 3121 [F 2121 > http /	IN, ACK IN, ACK		
15 1.62205 16 1 62205 ■ Ethernet II, ■ Destinatio ■ Source: De Type: IP (■ Internet Pro ■ User Datagra Source por Destinatio Length: 58 Checksum	bytes on wire, 92 bytes bytes on wire, 92 bytes src: Dell_00:6c:cd on: Broadcast (ff:ff: 11_00:6c:cd (00:19:b) 0x0800) tocol, src: 193.48.20 m Protocol, Src Port t: netbios-ns (137) n port: netbios-ns (1 0x0feb [correct]	193.51.224.23 193.48.200.198 193.51 224 22 193.48.200.198 193.51 224 22 193.48.200.198 193.51 224 23 193.48.200.198 193.51 224.23 193.51 224.23 193.48.200.198 193.51 224.23 193.48.200.198 193.51 224.23 193.48.200.198 193.51 224.23 193.48.200.198 193.48.200 193	DST: Bri 20), DST	3121 > http 1 http > 3121 [F 3121 > http 1 oadcast (ff:ff: : 193.48.200.25 : netbios-ns (1	TN, ACK TN, ACK TN, ACK TR, ACK TF: FF: FF 5 (193.4 37)		Pa
15 1.62205 16 1.62205 ■ Ethernet II, ■ Destinatio ■ Source: De Type: IP (■ Internet Pro ■ User Datagra Source por Destinatio Length: 58 Checksum:	<pre>1 193.40.200.193 2 193.51.224.23 5 193.48 200 193 bytes on wire, 92 bytes or: pell_00:6c:cd (n: Broadcast (ff:ff:1 11_00:6c:cd (00:19:b) 0x0800) tocol, Src: 193.48.20 m Protocol, Src: 193.48.20 m Protocol, Src: 193.48.20 n port: netbios-ns (137) n port: netbios-ns (137) n port: netbios-ns (137) ff ff ff 00 19 b2 0 </pre>	193.51.224.23 193.48.200.198 193.51 224 22 res captured) (00:19:b9:00:6c:cd), ff:ff:ff:ff) 9:00:6c:cd) 00.120 (193.48.200.1 : netbios-ns (137), 137)	DST: Br 20), DST DST Port	3121 > http : http > 3121 [F 3121 > http oadcast (ff:ff: : 193.48.200.25 : netbios-ns (1	TN, ACK TN, ACK TN, ACK TR 5 (193.4 37)		Pa
15 1.62205 16 1.62205 ■ Ethernet II, ■ Destinatio ■ Source: De Type: IP (■ Internet Pro ■ User Datagra Source por Destinatio Length: 58 Checksum: 4 0000 FF FF FF 0010 00 4e 5f 0020 c8 ff 00	bytes on wire, 92 bytes of the second of the s	193.51.224.23 193.48.200.198 193.51 224 22 res captured) (00:19:b9:00:6c:cd), ff:ff:ff:ff) 9:00:6c:cd) 00.120 (193.48.200.1 : netbios-ns (137), 137) 0 6c cd 08 00 45 00 2 cl 30 c8 78 cl 30 8 88 2a 01 10 00 01	DST: Br 20), DST DST Port	<pre>3121 > http :</pre>	TN, ACK TN, ACK TN, ACK TR 5 (193.4 37)		Pa
15 1.62205 16 1 60205 16 1 60205 16 1 60205 16 1 60205 16 1 60205 16 1 60205 16 1 60205 17 500762 De Type: IP (10 Ternet Pro 10 User Datagra Source por Destinatio Length: 58 Checksum: 10 00 f1 f4 f5 10 00 68 ff 00 10 00 68 ff 00	193.40.200.193 2 193.51.224.23 5 193.42.200.103 bytes on wire, 92 bytes src: Dell_00:6c:cd () n: Broadcast (ff:ff:1 100:6c:cd (00:19:b) 0x0800) tocol, src: 193.48.20 m Protocol, Src Port t: netbios-ns (137) n port: netbios-ns (: 0x0feb [correct] Ff ff ff ff (00.19 b) 0 43 00 00 80 11 c7 8 89 00 89 00 3a 0f e 00 00 80 11 c7 8	193.51.224.23 193.48.200.198 193.51 224 22 193.48.200.198 193.51 224 22 193.48.200.198 193.51 224 22 193.48.200.198 193.51 224 23 193.51 224 23 193.54 23 193.54 20 193.54 20 193.55 20	Dst: Br 20), Dst Dst Port	3121 > http > 3121 [F http > 3121 [F 3121 > http > 3121 > http > 3121 > http > 3121 > http 3121 >	FF:ff:ff 5 (193.4 37)		Pa

La fenêtre est divisée en trois parties.

1. La **première partie** est de type général, on y trouve des informations de type adresse IP des machines ou encore protocole utilisé lors de l'échange des données.

2. La **deuxième partie** de la fenêtre reprend ici la trame sélectionnée et la détaille soit dans les sept couches du modèles OSI ou dans les quatre couches du modèle IP. Pour plus d'informations à ce sujet des tutoriaux sont disponibles sur le net.

3. La troisième et dernière partie est une vision de la trame en codage hexadécimal et ASCII

Nous allons voir maintenant comment capturer les trames sur le réseau sur lequel le sniffer est connecté.

Etape 2 : Capture de trames sur le réseau

Pour capturer les trames sur le réseau, vous devez allez dans le menu *"Capture"* et cliquez sur "Start". La fenêtre suivante s'ouvre.

UFR de Mathématiques et Informatique

Interface: Br IP address: 193	oadcom NetXtre	eme Giga	abit Ethernet Driver (Mic	rosoft's Packet Scheduler) : \Device'
Capture pack	r type: Ethe			megabyte(s) Wireless Settings
Limit each pa	cket to 68		bytes	
⊆apture Filter:				
Capture File(s)				Display Options
File:			Browse	Update list of packets in real time
🔲 Use multiple f	iles			1271
Next file eve	y 1		🗘 megabyte(s) 🖂	Automatic scrolling in live capture
🔄 Next file eve	γ 1		🗘 minute(s) 🗠	Hide capture info dialog
💌 Ring buffer v	ith 2		🗘 files	Mana Davah kina
Stop capture	after 1		🗘 file(s)	
Stop Capture	20			Enable MAC name resolution
🔲 after	1	0	packet(s)	Enable network name resolution
🔲 after	1	0	megabyte(s) 😪	
🔲 after	1	0	minute(s) ~	Enable transport name resolution

Choisissez l'interface sur laquelle vous voulez "écouter" le trafic. Si vous en avez qu'une le choix ne sera pas très difficile.

Par défaut l'espace réservé à la collecte des données est défini à 1MB. Cela devrait être suffisant. Dans le cas contraire augmentez-le.

Activer l'option "**Capture packets in promiscuous mode**". Cette option permet à la carte réseau de lire et d'intercepter tout le trafic sur le réseau. Dans le cas contraire celle-ci n'interceptera que les trames qui lui sont destinées et ainsi vous ne verrez pas toutes les trames Multicast et Broadcast.

Laissez le champ "**Capture Filter**" vide dans un premier temps. Nous verrons par la suite comment le remplir. Nous ne toucherons pas non plus aux autres options.

Il ne vous reste plus qu'à démarrer la capture en cliquant sur "OK". La fenêtre suivante s'ouvre.

🖪 Wireshark: Capt	ture from Broadcom N	NetXtreme Gigabit Et	ihernet 🔳 🗖 🔀
Captured Packets			
Total	0	% of total	
SCTP	0		0.0%
TCP	0		0.0%
UDP	0		0.0%
ICMP	0		0.0%
ARP	0		0.0%
OSPF	0		0.0%
GRE	0		0.0%
NetBIOS	0		0.0%
IPX	0		0.0%
VINES	0		0.0%
Other	0		0.0%
Running	00:00:17		
	S	top	

Capturez environ 30 secondes de trafic entre le poste client et serveur. Puis cliquez sur "Stop". *Wireshark* va alors afficher les trames capturées par votre carte réseau dans un format lisible ci -dessous.

Eile	Edit	⊻iev ©) Ga	o <u>⊂</u> X	aptur	e į	Analy	ze	Statis	tics X	Help	Æ	5 1	٩		¢2	\$	Ŕ	7	7	Ŧ	1
Eilter:											3710	200	- 1	- Carero		•	Expre	essior	- 	⊆lear	Appl	y
No		Time			Sc	ource	1				D	estina	ation				Pr	otocc	l I	nfo		^
	1 2 3 4	0.00	0725 .345 9817	0 2 4 8	1 8 1 2	92. 6.6 92. 09.	168 4.1 168 85.	.0. 45. .0. 137	3 148 3 .147	,	8 1 2 1	6.6 92. 09. 92.:	4.1 168 85.3 168	45. .0. 137 .0.	148 3 .14 3	7	D D T T	NS NS CP CP	and with	tan tan 158 ittp	dan d dan d > h > 3	
	5 6 7 8	0.19 0.22 0.29	827 497 404	0 7 3 3	19 19 20	92. 92. 99.	168 168 85.	.0. .0. 137	3 3 .147 147	2	2211	09. 09. 92.: 92.:	85.1 85.1 168	137 137 .0.	.14 .14 3 3	7 7	T H T T	CP TTP CP	3 0 1	158 ET ttp	א < רא / HT אפג <	
	9 10 11	1.08	384 389 3403	5 5 6	20	09. 92.: 92.:	85. 168 168	137 .0. .0.	.147 .147 3 3	*	1 2 2	92.: 09. 09.	168 85.: 85.:	.0. 137 137	3 .14 .14	7 7	T(T) T(CP CP CP	[3 [TCP 158 TCP	sec > h Wir	
	12 13 14	1.08 1.19 1.19 1.19	428 479 500	9 4 1 6	20 20 19	09. 09. 92.:	85. 85. 168 168	137 137 .0.	.147 .147 3 3	, ,	1 2 2 2	92.: 92.: 09.	168 168 85.1 85	.0. .0. 137	3 3 .14 14	7	T T T T	CP CP CP	[TCP TCP 158	sec sec > h	
<	ĨŔ	1 19	601	1	5	na I	25 25	127	145	,	ĩ	a7 .	168	0	3		τı	-0	ř	TCD	C D C	~
∓ Fr ∓ Et ∓ Ir	ame ther	e 1 (net net	74 II, Pro	byt sr toc	es c: ol,	on Int Sr	wir el_ c:	e, 90: 192	74 k 7a:8 .168	oyte 3a (3.0.	s c 00: 3 (apt 0e: 192	ure 35: .16	d) 90: 8.0	7a:	8a) , D:	, Ds st:	t: 86.	Dra 64.:	ytek 145.	_26 148	*
+ US	ser	Data	igr a	m P	rot	0C0 7	1,	src	Por	rt:	302	7 (302	7),	Ds	t Pi	ort:	do	mai	n (5	3)	
)000)010)020)030)040	00000	0 50 0 3c 1 94 0 00 c 65	7f 7e 0b 00 02	26 e6 d3 00 66	fe 00 00 00 72	cf 00 35 00 00	00 80 00 04 00	0e 11 28 6e 01	35 13 34 65 00	90 4b bb 77 01	7a c0 80 73	8a a8 c9 06	08 00 01 67	00 03 00 6f	45 56 00 6f	00 40 01 67	., : j,	⊃.&. <~	5. (5. .K 4. ew	z 	E. V@

Sur la première partie de cette fenêtre les différentes trames capturées s'affichent et suivant les colonnes nous avons les informations suivantes:

Première colonne : numéro de la trame.

Deuxième colonne : temps écoulé depuis le départ de la capture et l'arrivée de la trame.

Troisième colonne : adresse IP ou nom de la machine émettrice

Quatrième colonne : adresse IP ou nom de la machine réceptrice

Cinquième colonne : protocole utilisé entre les deux machines

Sixième colonne : informations complémentaires

La quantité de données capturées peut vite devenir considérable, d'autant plus que plusieurs communications peuvent êtres établies en parallèle comme par exemple une connexion à <u>www.google.fr</u> et une autre à <u>www.tplpc.com</u>.

C'est pourquoi nous allons voir comment définir un filtre pour capturer une partie de tout ce que voit la carte réseau.

Etape 3 : Les filtres

Il y a deux sortes de filtres. Les filtres à la capture et les filtres à l'affichage. Ces filtres n'ont pas la même syntaxe. Pour Unix la syntaxe des filtres à la capture est la même que les filtres utilisés pour la commande tcpdump. Pour en connaitre le format, il faut donc utiliser man tcpdump. Quand aux filtres à l'affichage, la

syntaxe est une syntaxe propriétaire à Wireshark. Pour en connaître la syntaxe, il faut utiliser la commande man wireshark. La section présente donne des exemples pour ces deux types de filtres.

1. Filtres de capture

Ne seront conservés que les paquets pour lesquels le filtre est vrai. Les filtres se décomposent en 3 parties :

- le protocole à capturer : exemples : ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp ou udp,
- l'identifiant qui peut être src ou dst,
- un champ qui peut être host, net ou port suivi d'une valeur.

Les opérateurs and, or et not peuvent être utilisés pour combiner des filtres.

Filtre	Fonction
host 172.16.0.1 and tcp	ne conserve que les paquets TCP à destination ou en provenance de la machine 172.16.0.1
udp port 53	ne conserve que les paquets UDP en provenance ou à destination du port 53
udp port 53 and dst host 172.16.0.1	ne conserve que les paquets UDP en provenance ou à destination du port 53 et à destination de la machine 172.16.0.1
tcp dst port 80 and dst host 172.16.0.1 and src net 172.16.0.0 mask 255.255.255.0	ne conserve que les paquets TCP à destination de la machine 172.16.0.1 sur le port 80 et en provenance des machines du sous-réseau 172.16.0/24

2. Filtres d'affichage

Les filtres d'affichage sont un peu plus fins que ceux de la capture. Seuls les paquets pour lesquels l'expression du filtre est vraie seront gardés. Les expressions sont basées sur les champs disponibles dans un paquet. Le simple ajout d'un champ veut dire que l'on garde le paquet si ce champ est disponible. Maintenant, on peut aussi utiliser les opérateurs ==, !=, >, <, >= et <= pour comparer les champs avec des valeurs. Les expressions ainsi fabriquées peuvent être combinées avec les opérateurs && (pour un et logique), || (pour un ou logique), ^^ (pour le ou exclusif) et ! Pour la négation. L'usage des parenthèses est possible.

Voici quelques exemples de champs disponibles

Champ	Туре	Signification
ip.addr	adresse IPv4	adresse IP source ou destination
ip.dst	adresse IPv4	adresse IP destination
ip.flags.df	booléen	Drapeau IP, ne pas fragmenter
ip.flags.mf	booléen	Drapeau IP, fragments à venir
ip.ttl	entier non signé sur 8 bits	Time to live
nbdgm.src.ip	adresse IPv4	adresse IP source d'un paquet Netbios Datagram
nbdgm.src.port	entier non signé sur 16 bits	port IP source d'un paquet Netbios Datagram
http.request	booléen	requête HTTP
http.response	booléen	réponse HTTP
icmp.code	entier non signé sur 8 bits	numéro du code d'une commande ICMP
icmp.type	entier non signé sur 8 bits	numéro du type d'une commande ICMP
ftp.request	booléen	requête FTP
ftp.request.command	chaine de caractères	commande FTP
ftp.reponse.data	chaine de caractères	donnée de transfer FTP
dns.query	booléen	requête DNS
dns.response	booléen	réponse d'une requête DNS

Voici quelques exemples de filtres

Filtre	Signification
ip.addr == 172.16.0.100	tous les paquets IP en provenance ou à destination de la machine

	172.16.0.100
(ip.addr == 172.16.0.100) (dns.response)	&& tous les paquets IP en provenance ou à destination de la machine 172.16.0.100 qui sont des réponses à des requêtes DNS
(ip.addr >= 172.16.0.100) (ip.addr <= 172.16.0.123)	&& tous les paquets IP en provenance ou à destination des machines comprises entre l'adresse IP 172.16.0.100 et l'adresse IP 172.16.0.123 (comprises)

3. Comment définir un filtre pour la capture des trames (Capture Filter)

Allez dans le menu "Capture". Puis cliquez sur "Capture Filters".La fenêtre suivante s'ouvre.

Considérons que notre machine a l'adresse IP 192.168.1.33.

Nous voulons capturer uniquement les trames échangées entre celle-ci et la machine avec l'adresse IP 145.200.80.45.

Pour cela cliquez sur "New".

Dans le champ "Filter Name" entrez le nom de votre filtre : mon filtre (par exemple).

Dans le champ "Filter string" entrez la chaîne suivante : host 145.200.80.45. Cliquez maintenant sur "save" et voilà votre filtre est défini vous pouvez cliquez sur "close" pour fermer la fenêtre.

Retournez dans le menu "Capture" et cliquez sur "Start". Reprenez les mêmes options que précédemment. Cliquez sur le bouton "Capture Filter" et sélectionnez votre filtre. Voilà cliquez sur "OK" pour démarrer la capture avec le filtre en question.

Pour plus de détail sur la structure des filtres vous pouvez consulter l'aide en appuyant sur la touche F1 et en allant sur l'onglet "Capture Filter"

L3 - Réseaux & Télécommunications TD n°6

UFR de Mathématiques et Informatique

🔼 (Untitle	d) – Wiresh	ark			
<u>Eile E</u> dit	⊻iew <u>G</u> o	apture <u>A</u> nalyze Stat	istics Help		
		₩ © 🖬	× • 🖉 🖉 🗢		
Eilter:				Expression <u>C</u> lear App	yly
No T	me	Source	Destination	Protocol Info	^
10	.000000	192.168.0.3	86.64.145.148	DNS Standar	d query A
3 0	Wires!	hark: Capture Filter	. 192.100.0.9		http [SYN]
5 0 6 0 7 0 8 1 9 1 10 1 11 1 12 1 13 1 14 1 15 1 15 1 15 1 15 1 15 1 15 1 15	Edit New Delete	Filter Ethernet address 00:08 Ethernet type 0x0806 (No Broadcast and no Mu No ARP IP only IP address 192.168.0.1 IPX only TCP only UDP only TCP or UDP port 80 (HT HTTP TCP port (80) No ARP and no DNS Non-HTTP and non-SMT	: 15:00:08:15 ARP) Jlticast TP) P to/from www.wireshark.org	58 > 57 / H tp > 58 > 58 > 58 > 58 > 58 > 58 > 58 > 58	http [ACK] TTP/1.1 3158 [ACK] gment of a dment of a http [ACK] ndow Updat gment of a http [ACK] ndow Updat coment of a http [ACK] sife:cf (0 3 (86.64.1)
0010 00 0020 91	Filter name	e: Ethernet address 00:08	3:15:00:08:15	. К 41	. V@-
0030 00 0040 6c	Filter strin	g: ether host 00:08:15:00	0:08:15	ews.g	oog
User Datagram	Help		<u>o</u> k	Gancel	

Une autre méthode consiste à capturer toutes les trames dans un premier temps et de filtrer par la suite. L'avantage de cette solution est d'avoir toujours la capture de départ et d'y appliquer par la suite autant de filtres que l'on souhaite. C'est ce que nous allons voir dans le prochain chapitre.

4. Comment définir un filtre pour la visualisation des trames (Display Filter)

Essayons d'appliquer le même filtre que précédemment. Dans un premier temps faites une capture sans appliquer de filtre (reportez vous au premier paragraphe). Stoppez la capture. Allez sur la barre FILTER et sélectionner « EXRESSION ». une fenêtre s'ouvre vous permettant de rédiger des flitres d'affichage Par exemple on sélectionne le protocole Ethernet et l'adresse source. On tape la chaîne suivante : eth.src==12:23:45:67:34 5A et on valide. Voilà le filtre d'affichage est appliquez. Si vous voulez le sauvegarder cliquez sur "Save".

Si maintenant vous voulez l'annuler, effacez la chaîne dans le champ "Filter string" ou cliquer sur « CLEAR ».

L3 - Réseaux & Télécommunications TD n°6

UFR de Mathématiques et Informatique

Eilter;	udp and ip.addr==193.51.25.229	+	Expression Clear Apply
No	Time Source Dest 1 0.000000 192.168.0.3 86. 2 0.107252 86.64.145.148 192 2 0.112454 102.168.0.3 200	ination 64.145.148 .168.0.3	Protocol Info DNS Standard que DNS Standard que
	Field name	Relation	Value (Ethernet or other MAC addres
	ESS ETHERIC	==	Predefined values:
	 ETHERIP Ethernet eth.dst - Destination (Destination Hardware Addrese) 	>= >=	
K E F	eth.src - Source (Source Hardware Address) eth.len - Length	<= contains	
⊞E ⊞I ⊞U	eth.type - Type eth.addr - Address (Source or Destination Hardwa eth.trailer - Trailer (Ethernet Trailer or Checksum)	matches	
< 0000	eth.ig - IG bit (Specifies if this is an individual (unic		Range (offset:length)

Etape 4 : sauvegarde d'un résultat de capture

Pour sauvegarder le résultat d'une capture dans un fichier, il faut sélectionner la commande « Save as » dans le menu « File ». Une fenêtre nous proposer de choisir le répertoire et le nom du fichier, ainsi que le format/type de fichier de sauvegarde (conserver le format par défaut libpcap).

Pour n'enregistrer qu'une trame ou un une sélection de trames, vous avez a votre disposition ces options dans le menu « Packet Range ».

UFR de Mathématiques et Informatique



Etape 5 : Répondre aux questions suivantes :

5.1 Lancer les machines virtuelles client et Serveur

5.2 taper sur la console du serveur la commande « ifconfig » (voir le manuel man pour la syntaxe de la commande ifconfig). Identifier les adresses Ethernet du serveur. Identifier les adresses IP du serveur. Réitérer la même opération avec le poste client.

5.3 sur le poste Serveur, lancer le logiciel Wireshark sur votre interface Ethernet (eth0),

5.4 sur le poste client, taper une commande de type « ping » à destination du serveur et capturer environ 30 secondes de trafic sur le poste serveur (voir le manuel man pour la syntaxe de la commande ping). Enregistrer le résultat dans un fichier « test ».

5.5 Combien de trames avez-vous capturé ?

5.6 Analyser la première trame Ethernet et reporter les valeurs des champs de contrôle de cette trame dans un tableau. Quelle information cette trame transporte t elle ?

5.7 Recherchez sur Internet le document RFC 1700. Quelle information mentionne t il en relation avec la trame Ethernet ?

5.8 Au moyen des filtres d'affichage sélectionner uniquement les trames dont l'émetteur est le poste client (sur la base de son adresse Ethernet).

5.9 Décrivez la procédure (commandes systèmes, filtres wireshark) permettant de capturer et de filtrer les trames Ethernet transportant uniquement un paquet ARP ayant pour origine (émission) le poste serveur.