

# **ETUDE D'UN RESEAU INFORMATIQUE**

## Support : Réseau informatique

## Pré requis (l'élève doit savoir):

• Savoir utiliser un ordinateur

#### **Programme**

## **Objectif terminale :**

L'élève doit être capable de réaliser le montage d'un réseau et de le paramétrer

## Matériels :

• Logiciel wireshark, Cisco Packet Tracer

## 1. <u>Questions</u>

• A quoi peut servir un réseau informatique

• Expliquer son principe de fonctionnement

Nom :....

Prénom :....

• Quels sont les différents types de topologie de réseau

• Qu'est-ce un masque de sous réseau, à quoi ça sert ?

• Qu'est-ce une adresse mac ?

• Qu'est-ce une adresse IP ?

• Quels sont les éléments importants dans les adresses pour que deux ordinateurs puissent communiquer sur un même réseau.

• Donner le nom et la fonction des différents éléments qu'on peut trouver dans un réseau

Nom :	
-------	--

Prénom :....

## 2. <u>Manipulation (indiquer la commande réseau qui vous a permis d'obtenir le résultat)</u>

- Donner l'adresse IP de votre ordinateur et le masque de sous réseau
- Donner la classe du réseau local (A, B, C, D) et expliquer votre réponse
- Donner l'adresse mac

Prénom :....

• Donner l'adresse IP d'au moins deux ordinateurs branchés sur le réseau

a. Etude protocole Arp

- Depuis votre terminal avec l'invite de command (cmd), vider le cash de la table arp : arp -d
- Dans un terminal, affichez la table ARP (capturer la table et la coller sur le TP)

Exemple :

C:\Windows\system32>a	rp -a	
Interface : 192.168.1	.17 Øxc	
Adresse Internet	Adresse physique	Туре
192.168.1.1	34-8a-ae-21-75-d2	dynamique
192.168.1.10	fØ-82-61-36-83-92	dynamique
192.168.1.15	24-0a-64-80-47-69	dynamique
192.168.1.255	77-77-77-77-77	statique
224.0.0.2	01-00-5e-00-00-02	statique
224.0.0.22	01-00-5e-00-00-16	statique
224.0.0.251	01-00-5e-00-00-fb	statique
224.0.0.252	01-00-5e-00-00-fc	statique
224.0.0.253	01-00-5e-00-00-fd	statique
239.255.255.250	01-00-5e-7f-ff-fa	statique
255.255.255.255	<u> </u>	statique

- Pinguer sur une machine du réseau qui n'est pas encore dans la table ARP.
- Afficher la nouvelle table ARP, que constatez-vous ?

## b. Etude protocole IMCP

- Dans Capture/Option, remplissez les champs :
- Interface
- Capture Filter (icmp and ip src host (adresse ip ordinateur source))
- Enable network name resolution
- Démarrez la capture

Nom :		Prénom :	
🚄 Wi	reshark: Capture Options	A DESCRIPTION	
Сар	iture		
C	apture Interface	Link-layer header Prom. Mod	e Snaplen [B] Buffer [MiB] Capture Filter
	Connexion réseau sans fil 2 fe80:fdf5:7f35:ddde:6ble 0.0.0.0	Ethernet enabled	262144 2 icmp and ip src host 192
	Connexion réseau Bluetooth		<b>•</b>
		m	4
	Capture on all interfaces		Manage Interfaces
	Use promiscuous mode on all inter	faces	
	apture Filter: icmp and ip src host :	192.168.1.17	Compile selected BPFs
Cap	oture Files		Display Options
Fi	ile:	Brows	e Update list of packets in real time
	Use multiple files	V Use ncan-ng format	Automatically scroll during live capture
	Next file every 1	megabyte(s)	☑ <u>H</u> ide capture info dialog
	Next file every	minute(s)	Name Resolution
	Ring buffer with 2	files	✓ Resolve MAC addresses
Stop	p Capture Automatically After		Resolve <u>n</u> etwork-layer names
	1 packet(s)	1 megabyte(s)	
	1 file(s)	1 minute(s)	Use <u>e</u> xternal network name resolver
	Help		<u>Start</u>

- Dans une fenêtre de terminal, lancez la commande ping www.google.fr pendant quelques secondes.
- Cliquez sur Stop
- Analysez les trames :
  - o Quelle est l'adresse MAC de l'interface réseau du serveur google?
  - o Quelle est la taille d'un paquet en octets?
  - Quelles sont les adresses IP source et destination?

```
    B Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 3
    B Ethernet II, Src: Azurewav_a7:97:88 (1c:4b:d6:a7:97:88), Dst: Sagemcom_21:75:d2 (34:8a:ae:21:75:d2)
    □ Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 173.194.78.94 (173.194.78.94)

                     Version: 4
                     Header Length: 20 bytes
          B Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
                     Total Length: 60
                    Identification: 0x02d1 (721)
          ⊞ Flags: 0x00
                   Fragment offset: 0
                   Time to live: 128
Protocol: ICMP (1)
          ⊞ Header checksum: 0x7a16 [validation disabled]
                                                          pc5.home
                                                                                                          (1)

        34
        8a
        ae
        21
        75
        d2
        1c
        4b

        00
        3c
        0.2
        d1
        0.0
        0.0
        80
        01

        4e
        5e
        0.8
        0.0
        4d
        52
        0.0
        0.1

        67
        68
        69
        6a
        6b
        6c
        6d
        6e

        77
        61
        62
        63
        64
        65
        66
        67

0000
0010
0020
0030
0040

        d6
        a7
        97
        88
        08
        00
        45
        00

        7a
        16
        c0
        a8
        01
        11
        ad
        c2

        00
        09
        61
        62
        63
        64
        65
        66

        6f
        70
        71
        72
        73
        74
        75
        76

        68
        69

                                                                                                                                                                                                                                                                                     4...!u..K .....E.
.<.....Z.
N^...R....abcdef
ghijklmn opqrstuv
wabcdefg hi
```

 Calculer chaque adresse en hexadécimal (détailler les calculs) et la comparer à la valeur affichée sur wireshark

Exemple :

192.168.1.17 => c0 a8 01 11

Nom :	
Remarque :	

Selon votre capture, il peut être utile d'appliquer un filtre qui ne va afficher que certains paquets.

Donc pour mettre en place un filtrage (par exemple pour n'afficher que les paquets dont l'adresse source est 192.168.200.21) il faut saisir le filtre dans la **section Filter** puis cliquer sur le bouton **Apply**:

Filter: ip.src == 192.168.200.21	Ŧ	Expression	Clear	Apply
----------------------------------	---	------------	-------	-------

Si le fond de la zone de saisie du filtre n'est pas vert, c'est qu'il y a une erreur de syntaxe.

Dans le cas d'un trafic ftp vous pouvez aussi dans le champ Filter saisir ftp puis cliquez sur Apply.

Un grand nombre de protocoles compris entre les couches deux et sept du modèle OSI est disponible. Ils peuvent être consultés quand vous cliquez sur le bouton "Expression ..." dans la fenêtre principal de Wireshark. Quelques exemples de protocole sont: IP, TCP, DNS, SSH.

🗖 Th	e Wir	eshark	Netw	ork Ana	lyze	H.											. 🗆 ×	1
Eile	<u>E</u> dit	⊻iew	<u>G</u> o	Capture	٨r	halyze	<u>S</u> tatis	tics	<u>H</u> elp									
	<b>i</b>	0	8	<b></b>		D	K	×	e,		9		¢1	⇔	۲	Ŧ	\$	
<u>F</u> ilter:					_					_		Ŧ	Ē	pression	<b></b>	]lear A	pply	
										l								
Ready	y to loa	d or ca.	No	Packets							۵P	=	٦M	A113	AK	(.50)	M 🕂	•

Wireshark: Filter Expression		
Field name	Relation	Value (protocol)
2dparityfec	is present	
	==	Predefined values:
	!	
802.11 MGT     802.11 MGT     1	>	
😟 802.11 Radiotap	<	
802.3 Slow protocols	>=	
± 9P	<=	
AAL1	contains	
AAL3/4	matches	
AARP		
ACAP		
I ACN	8	Range (offset:length)
openmaniak.com	A 🖸	QK <u>C</u> ancel

## Exemple de syntaxe de filtre :

#### ip.addr == 10.1.1.1

Affiche les paquets avec une adresse source ou destination de 10.1.1.1.

#### Nom :.....

#### Prénom :.....

#### ip.src != 10.1.2.3 or ip.dst != 10.4.5.6

Affiche les paquets avec une adresse IP source différente de 10.1.2.3 ou avec une adresse IP destination différente de 10.4.5.6.

#### Tcp.port==25

Affiche les paquets dont le port TCP source ou destination est égal à 25.

#### Tcp.dstport==25

Affiche Les paquets avec un port TCP de destination 25.

#### Comment analyser la capture réseau ?

On commence par charger la capture par le menu File > Open (/tmp/capture.pcap). Une fois le fichier chargé, on peut voir que la fenêtre de Wireshark est, par défaut, divisée en 3 sections:

- la première affiche une liste des paquets IP capturés
- la seconde donne le détail du paquet IP sélectionné dans la première section
- la troisième affiche le contenu (en hexadécimal) du paquet IP sélectionné dans la première section

Le volet du milieu affiche les détails de ce paquet. Les protocoles et les champs de protocole du paquet sélectionné sont indiqués. Ils s'affichent sous la forme d'une arborescence que vous pouvez développer ou réduire.

		eth1 - Wir	eshark	600000
File Edit View Go Capt	ure Analyze Statistics Telep	bony Tools Help		
	D; * 0 = Q =	··		R R 🖸 👹 🗹 📑 🚨 Liste des paquets
Filten		• Expression Clear	Apply	
No. Time	Source	Destination	Protocol	Info
	100.100.00.70	WJ.270.27.88	111.10	uci yudayyu damayo yu miyeyi.k
365 12.271613	192.168.29.79	83.243.19.11	HTTP	GET /decargn/bg_bandeau.gif HTTP/1.1
300 12.2/1/30	192.100.29.79	83.243.19.11	TUP	segment of a reassembled PDUJ
367 12.271790	192.168.29.79	03.243.19.11	UTTO	GET /smrite aif MTTO/1 1
308 12.273229	192.168.29.79	83.243.19.11	HITP	GET /Sprite.git Hilp/1.1
270 12 202472	100 50 148 20	192,108,29,1	661.42	Saruar Van Exchange Saruar Valla Bana
370 12 203472	103 168 20 70	192,100,23,75	TCD	A2046 > before [ACK] Care-71 Ach-1664 bire-11640 Lan-0 TEM-1404
371 12.233310	132.100.23.75	103 168 30 20	TEP	42040 > HELPS [ALK] SEQ-71 ALK-1004 WIN-11040 LEN-0 151-2494
372 12.254407	102 168 20 70	83 243 10 11	TCP	36890 > http [4(K] Seg-1 4/k-1 Win-5888 100-8 TSV-2494756 TS
374 12 294519	83 343 19 11	193 168 29 79	TCP	http > 36891 [SVN ACK] Sense Ark=1 Win=1468 Lense MSS=1468
175 12 294528	192 168 29 79	81 241 19 11	TCP	16891 > http: [ACK] Segn1 Acks1 Wins5888 Lenes TSVs2494756 TS
376 12, 294765	83, 243, 19, 11	192, 168, 29, 79	TCP	http > 36889 [SYN_ACK1 Sep=0 Ack=1 Win=1468 Len=0 MSS=1460
377 12,294774	192, 168, 29, 79	83, 243, 19, 11	TCP	36889 > http [ACK] Seg=1 Ack=1 Win=5888 Len=8 TSV=2494757 T5
378 12.295048	192, 168, 29, 79	83,243,19,11	HTTP	GET /favicon.ico HTTP/1.1
379 12,295153	192, 168, 29, 79	83,243,19,11	HTTP	GET /favicon.ico HTTP/1.1
<ul> <li>Ethernet II, Src: G-Prof</li> <li>Internet Protocol, Src:</li> </ul>	Com_77:25:c8 [80:0f:fe:77:25 192.168.29.79 (192.168.29.7	:c8), Dst: HewlettP_6 9), Dst: 192.168.29.1	4:6e:2c (00: (192.168.29	1f:29:04:6e:2c) .1)
<ul> <li>User Datagram Protocol.</li> </ul>	Src Port: 57865 (57865), Os	t Port: domain (53)		
* Domain Name System (que	rvì			
IResponse In: 11181				
Transaction ID: 8kald				
Finise (100 ab) exercis	of manual			
· Frags: exerce (Standa	in doeral			
Questions: 1				
Answer RRs: 0				
Authority RRs: 0				Détail du sa such offéntion of
Additional RRs: 8				Detail du paquet selectionne
Queries				
ing.achetezfacile.c	om: type A, class IN			
0000 00 1f 29 64 6e 2c 00	8f fe 77 25 c8 88 00 45 00	)dh		
0010 00 43 11 1f 40 00 40	11 6d ea c0 a8 1d 4f c0 a8	.C@.@. mO		and the second second second second
8829 1d 81 e2 89 66 35 68	2f bb el al d8 81 66 88 61			Contenu du paquet
10,50 108 00 80 80 80 60 60 03	69 63 67 03 61 63 68 65 74	1 mg.achet	-	112 CARL STATE OF THE STATE OF THE STATE OF
Frame (frame), 81 bytes	* Packets: 1833 Displaye	d: 1833 Marked: 0 Droppe	od: 0	- Profile: Default

#### Contenu du paquet :

La première colonne indique, avec 4 chiffres hexadécimaux, le rang du premier octet de la ligne courante dans la trame ;

La seconde affiche la valeur hexadécimale de 16 octets capturés à chaque ligne (un octet est représenté par deux caractères hexadécimaux) ;

La dernière représente à chaque ligne les caractères ASCII correspondants aux 16 octets de la seconde colonne (la correspondance n'est significative que lorsque du texte "imprimable" se trouve encodé dans ces octets).

Nom :.....

Prénom :....

c. Réalisation d'un réseau informatique

## Simulation :

• Installer le logiciel Cisco Packet Tracer

Nom	Modifié le	Туре	Taille
🍕 blank.pkt	09/09/2012 15:09	Cisco Packet Trac	1 Ko
🔁 Cisco Packet Tracer 6.2 for Windows Stud	25/08/2015 13:56	Application	150 207 Ko
french.ptl	09/09/2012 15:16	Fichier PTL	977 Ko
notice francaise.txt	09/09/2012 15:17	Document texte	1 Ko
🗾 Packet Tracer 4.11.pdf	09/09/2012 14:53	Adobe Acrobat D	4 570 Ko

• Modifier la langue voir notice

Nom	Modifié le	Туре	Taille
🍕 blank.pkt	09/09/2012 15:09	Cisco Packet Trac	1 Ko
🚏 Cisco Packet Tracer 6.2 for Windows Stud	25/08/2015 13:56	Application	150 207 Ko
french.ptl	09/09/2012 15:16	Fichier PTL	977 Ko
notice francaise.txt	09/09/2012 15:17	Document texte	1 Ko
🔁 Packet Tracer 4.11.pdf	09/09/2012 14:53	Adobe Acrobat D	4 570 Ko

 En suivant les instructions sur la vidéo (<u>http://www.sti2dsinhyrome.fr/video%20cisco%20packet%20tracer.html</u>), réaliser le réseau suivant et le tester

Rentrer les mêmes caractéristiques que le réseau de la salle, adresse ip de votre ordinateur et d'un autre ordinateur de la salle.



Nom :	
-------	--

Prénom :....

- Appeler professeur
- Refaire le montage en rajoutant un point d'accès wifi et un nouvel ordinateur connecté en wifi.
   Configurer le avec une sécurité WPA2 (clé : votre nom suivi de votre date de naissance, suivi nom lycée, Ex : dupont18101999hyrome)

