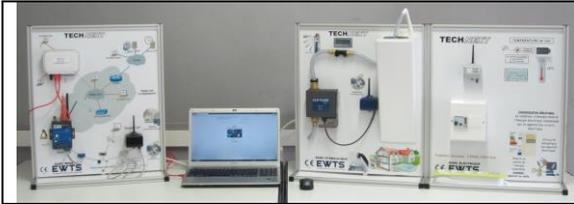


SYSTEME DE GESTION DES ENERGIES

EWTS

EMBEDDED WIRELESS TELEMETRY SYSTEM

Copyright **TECHNEXT**[®] 2012



Nom :
Prénom :
Classe :

 **Problématique:**
Comment accéder au serveur EWTS?

Activités du TP:

-  **1 Connexion au serveur (adressage IP)**
-  **2 Analyse du protocole HTTP**
-  **3 Ethernet et le protocole ARP**
-  **4 Synthèse**

Activité 1 : Connexion au serveur (adressage IP)

L'objectif est de connecter en réseau plusieurs postes de travail au serveur EWTS afin d'accéder aux données stockées par ce dernier.

La connexion physique au réseau

- Q1.** Quel est le type de topologie physique utilisé lorsque le PC et le serveur EWTS sont tous deux connectés au commutateur du banc de télémétrie ? Illustrer votre réponse en réalisant un schéma de ce réseau en supposant que tous les ports du commutateur sont utilisés pour connecter des ordinateurs et le serveur.

- Q2.** Quel type de cordon doit-on utiliser pour connecter le serveur EWTS au commutateur (croisé ou droit) ?

Plan d'adressage IP

L'objectif est de proposer, en se basant sur l'adresse IP et le masque de sous-réseau attribués au serveur, un plan d'adressage cohérent afin que les quatre ordinateurs puissent communiquer entre eux et avec le serveur.

Rque : Pour que deux machines connectées physiquement puissent communiquer directement entre elles, elles doivent posséder une adresse IP appartenant au même réseau. Le réseau est défini par l'adresse réseau et le masque de réseau.

Q3. Retrouver l'adresse réseau du réseau auquel appartient le serveur à partir de son adresse IP et du masque de sous-réseau qui lui est associé.

Il faut pour cela décomposer l'adresse IP du serveur et le masque de sous-réseau en binaire, puis effectuer une opération de ET logique entre cette adresse et le masque. Le résultat constitue l'adresse du réseau que l'on convertit en décimale pointée.

Pour rappel :

a	b	a ET b
0	0	0
0	1	0
1	0	0
1	1	1

E T	Adresse IP	192	.	168	.	3	.	127
		1 1 0 0 0 0 0 0 0	.	1 0 1 0 1 0 0 0 0	.	0 0 0 0 0 0 1 1	.	0 1 1 1 1 1 1 1
=	Masque	255	.	255	.	255	.	0
			.		.		.	
=	Adresse réseau		.		.		.	
			.		.		.	
	Adresse de diffusion		.		.		.	
			.		.		.	

Rque : L'adresse réseau ne peut pas être attribuée à une machine

Q4. Retrouver l'adresse de diffusion (broadcast) de ce réseau en complétant le tableau précédent

Rque : Cette adresse est utilisée pour envoyer des messages à toutes les machines du réseau (au sens IP du terme) en même temps. Elle ne peut pas non plus être attribuée à une machine.

Q5. A quelle classe d'adresse appartient l'adresse IP du serveur ?

Q6. Quel est le masque de sous-réseau par défaut pour cette classe ?

Q7. Quel est le nombre maximum de machines que l'on peut adresser sur ce réseau ?

Pour répondre à cette question, il faut compter le nombre de bits à 0 dans le masque de sous réseau. Le nombre maximum de machines est alors égal à :

$$n = 2^{\text{nombre_de_bits_a_0_dans_le_masque}} - 2$$

Rque : Le « -2 » à la fin de cette formule permet d'éviter de compter l'adresse réseau et l'adresse de diffusion qui ne peuvent pas être attribuées à une machine

Q8. A partir des informations précédentes, compléter le tableau résumé suivant :

Adresse IP du serveur	192.168.3.127
Masque de sous-réseau	255.255.255.0
Adresse réseau	
Adresse de diffusion (broadcast)	
Première adresse de la plage	
Dernière adresse de la plage	
Classe d'adresse	
Nombre de machines adressables	

Q9. En déduire le plan d'adressage en proposant une adresse IP pour chaque nœud du réseau (plusieurs solutions possibles)

Machine	Adresse IP
serveur	192.168.3.127
PC 1	
PC 2	
PC 3	
PC 4	

Configuration réseau du poste de travail

Q10. Réaliser le câblage réseau, si ce n'est déjà fait, en reliant l'ordinateur au commutateur (switch) à l'aide d'un cordon RJ45

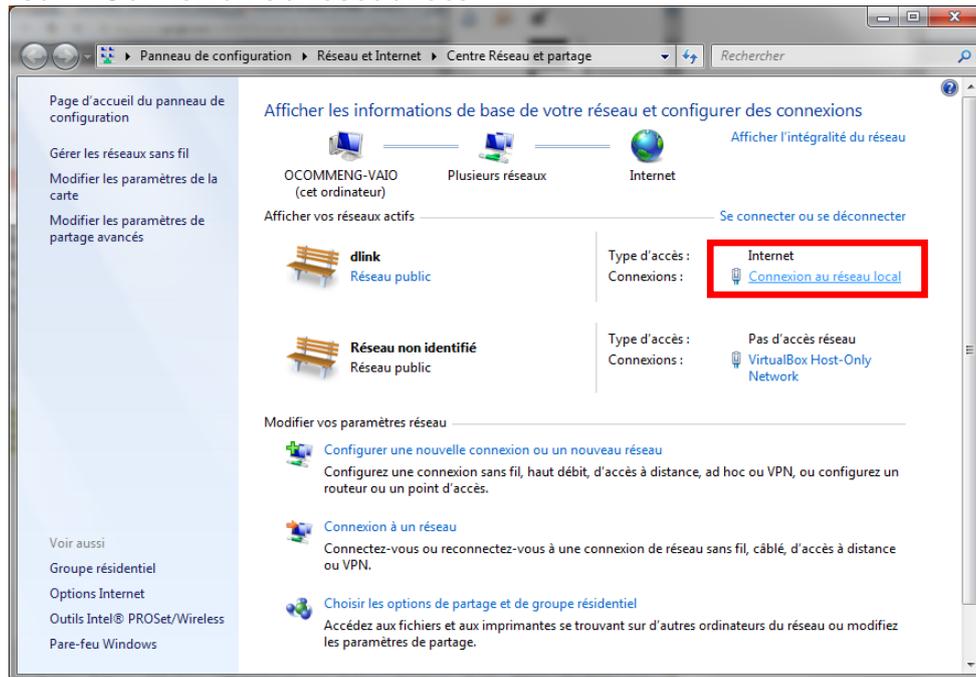
Q11. Attribuer un adresse IP et un masque de sous-réseau à la carte réseau du PC

Pour cela, sous Windows 7,

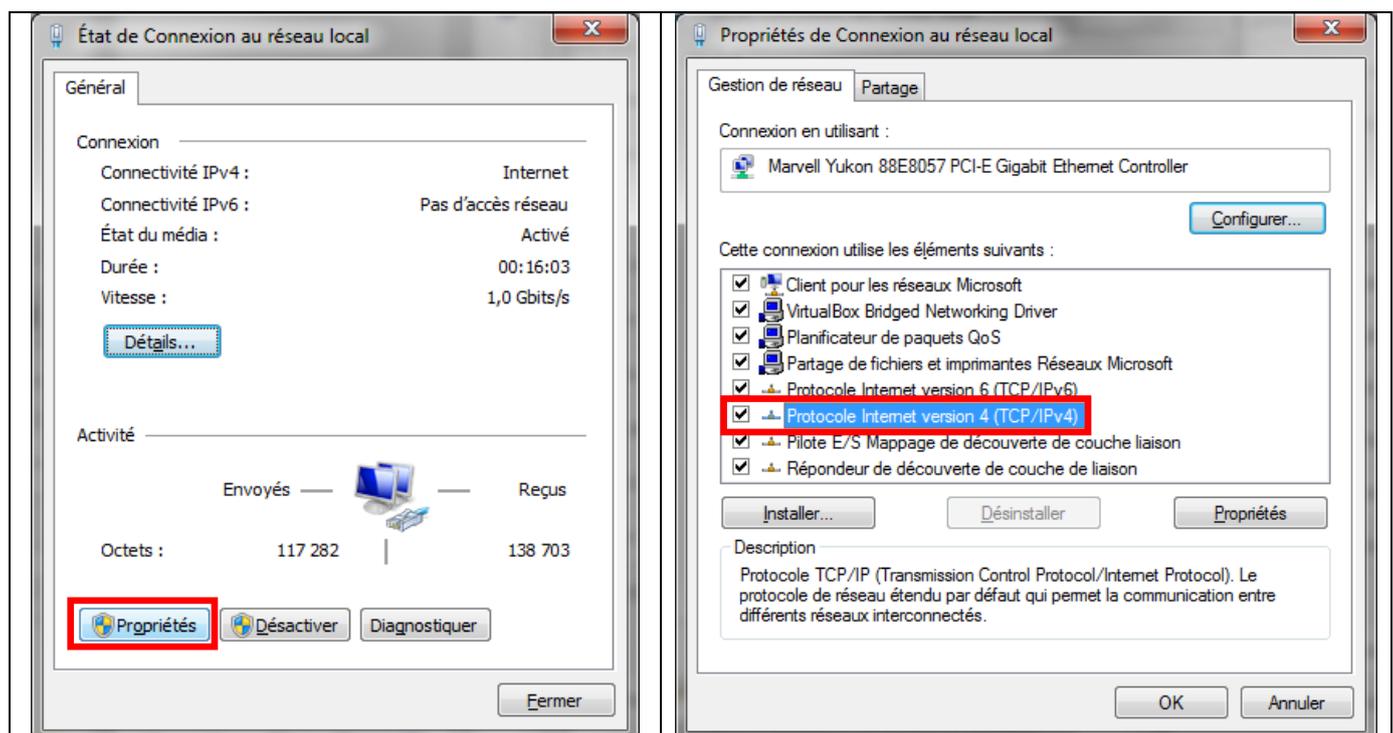
- repérer l'icône réseau en bas à droite de l'écran, faire un clic droit dessus, puis cliquer sur « Ouvrir le centre Réseau et partage »



- Cliquer sur « Connexion au réseau local »

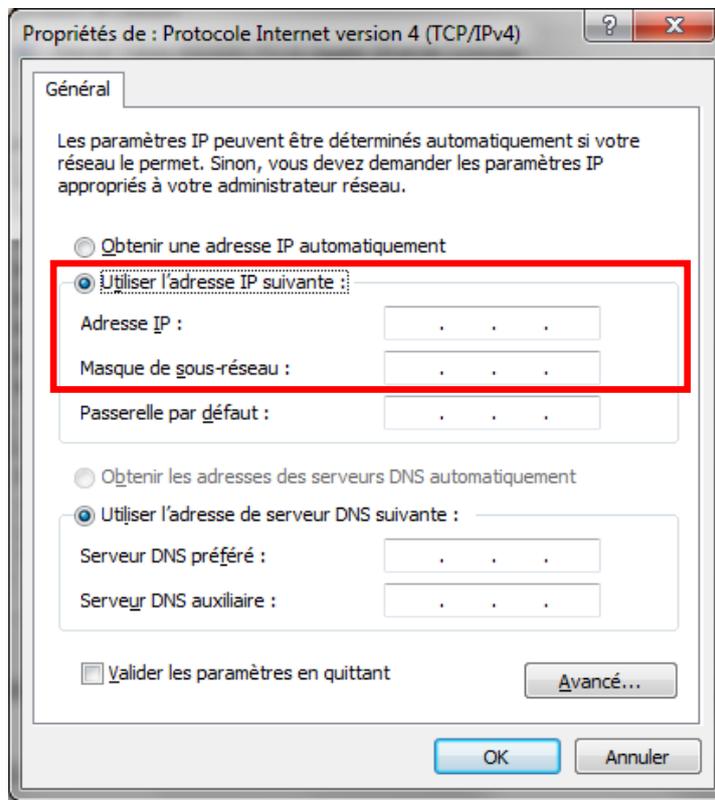


- Cliquer sur « Propriétés » puis double-cliquer sur « Protocole Internet Version 4 (TCP/IPv4) »



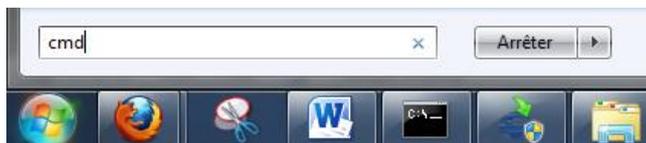
- Sélectionner la case « Utiliser l'adresse IP suivante » puis saisir l'adresse IP et le masque de sous réseau définis précédemment dans le plan d'adressage.

Rque : Attention, deux machines d'un même réseau ne doivent pas avoir la même adresse IP.



Rque : Dans notre cas il ne sert à rien de renseigner l'adresse de la passerelle par défaut car les PC et le serveur sont directement connectés ensemble grâce au commutateur. Ils appartiennent au même réseau (au sens IP) et n'ont donc pas besoin d'emprunter une passerelle pour communiquer entre eux.

- Bien fermer toutes les fenêtres afin que la nouvelle configuration soit bien prise en compte.
- Q12.** Vérifier que la configuration a bien été prise en compte à l'aide de la commande ipconfig
- Lancer l'invite de commande. Pour cela, ouvrir le menu « démarrer » (en bas gauche de l'écran) et saisir la commande « cmd » puis appuyer sur entrée



- Dans la fenêtre qui s'ouvre, lancer la commande « ipconfig »

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\ocommeng>ipconfig

Configuration IP de Windows

Carte Ethernet Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::186:4a31:1600:be7f%10
    Adresse IPv4. . . . . : 192.168.3.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte réseau sans fil Connexion réseau sans fil :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . : wappert.lyc-appert-44.local

C:\Users\ocommeng>
```

Test de la connectivité

Q13. Vérifier que la communication réseau avec le serveur est possible à l'aide de la commande « ping » (test de la connectivité)

- Pour cela, taper la commande « ping adresse_IP_serveur »

```
C:\Windows\system32\cmd.exe
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . . :

Carte Tunnel isatap.wappert.lyc-appert-44.local :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . :

C:\Users\ocommeng>ping 192.168.3.127

Envoi d'une requête 'Ping' 192.168.3.127 avec 32 octets de données :
Réponse de 192.168.3.127: octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.3.127:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\ocommeng>
```

Q14. En analysant le retour de cette commande, comment sait-on que la communication réseau avec le serveur est possible et donc que la connectivité réseau est bonne ?

Q15. Vérifier que la communication est possible avec les autres machines du réseau. Quelle commande avez-vous tapée ?

Activité 2 : Analyse du protocole HTTP

La configuration du système EWTS ainsi que l'accès aux valeurs et aux courbes de consommation s'effectue en chargeant une page web hébergée sur le micro-serveur. Le protocole de communication utilisé pour charger cette page est le protocole http (HyperText Transfer Protocol)

Q16. A quelle couche du modèle OSI appartient ce protocole ?

Q17. Capturer les échanges entre la machine client et le micro-serveur lors de la demande de chargement de la page d'accueil du système EWTS. Pour cela :

- Lancer le logiciel d'analyse de trafic réseau Wireshark.
- Lancer le navigateur web (firefox par exemple)
- Lancer la capture dans Wireshark
- Saisir l'adresse IP du serveur web dans la barre URL du navigateur
- Arrêter la capture dans Wireshark

Q18. Filtrer la capture de façon à ne conserver que la communication entre votre poste et le micro-serveur. Pour cela :

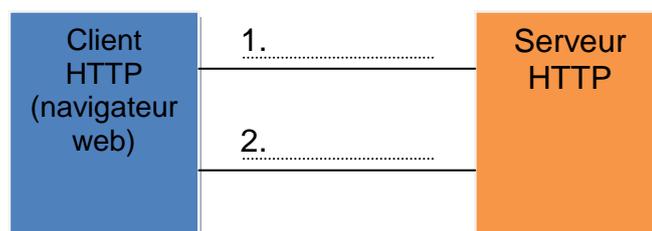
- Dans le champ « filter » ajouter : **http && ip.addr==192.168.3.127**

***Rque :** Le filtre précédent sert à visualiser uniquement les trames http échangées avec le serveur d'adresse 192.168.3.127*

- Cliquer sur « apply »

Q19. En regardant les colonnes « source » et « destination » (volet 1 de Wireshark) des deux premières trames filtrées, déterminer la chronologie de la communication HTTP en ajoutant sur le schéma suivant :

- Le sens de la communication
- La légende avec les termes suivants : **requête, réponse**



***Rque :** Ce schéma symbolise le principe du mode de communication Client-Serveur*

Q20. En regardant le champ « info » (volet 1 de Wireshark), noter la requête HTTP transmise par le client.

***Rque :** Dans la requête précédente, la ressource demandée est /, c'est-à-dire la page par défaut à charger lorsqu'on interroge le serveur par son adresse IP.*

Q21. Toujours à l'aide du champ « info », noter la réponse du serveur

Rque : La valeur 200 retournée par le serveur est un code de réponse signifiant qu'il est en mesure de retourner la ressource demandée (OK). Lorsque le serveur ne trouve pas la ressource demandé, il retourne le code 404 (page not found).

Q22. Que contient le champ data (Lined-base text data) (volet 2 de Wireshark) de la réponse http du serveur ?

Rque : La page reçue est en fait un cadre destiné à contenir plusieurs autres pages web. Ainsi, lorsque le navigateur reçoit le code de cette page, après l'avoir analysé, il émet de nouvelles requêtes HTTP pour charger ces pages supplémentaires

Q23. L'option « server » de l'en-tête HTTP de la réponse permet de connaître le type de serveur web qui répond. En observant ce champ dans le volet 2 de Wireshark, Quel logiciel fait office de serveur web sur le serveur EWTS ? Avec quel système d'exploitation ?

Q24. En observant la capture Wireshark des échanges, retrouver les deux requêtes suivantes émises par le navigateur. En déduire le nom des deux autres pages web (possédant une extension .html) que demande le navigateur.

Activité 3 : Ethernet et le protocole ARP

Les adresses physiques

Q25. Relever l'adresse MAC (adresse physique) de la carte ethernet de votre poste de travail. Pour cela :

- Ouvrir une fenêtre « Invite de commande » (menu démarrer -> exécuter -> cmd)
- Taper la commande **ipconfig /all**
- Relever la valeur du champ « adresse physique » de la carte concernée.

Adresse MAC :

Q26. Comment peut-on décomposer cette adresse ?

Partie _____.	Partie _____.

Q27. Retrouver le constructeur de la carte ethernet du poste de travail. Pour cela :

- Accéder au site <http://standards.ieee.org/regauth/oui/index.shtml>
- Saisir le code constructeur de la carte en respectant le format suivant : XX-XX-XX

Constructeur de la carte :

La table ARP

Chaque système communicant sur un réseau de type Ethernet tient à jour une table dynamique permettant d'associer l'adresse IP d'une machine, avec laquelle il désire ou il a déjà communiqué, à l'adresse physique vers laquelle transmettre la trame. Cette table s'appelle la table ARP ou cache ARP

Q28. A l'aide de la commande **arp -a**, afficher le contenu de la table arp. Combien d'entrées y-a-t-il ?

Q29. Vider le cache arp. Combien d'entrée contient la table à présent ? Pour cela :

- Ouvrir l'invite de commande en mode administrateur :
 - Menu démarrer -> Tous les programmes -> Accessoires -> clic droit sur « Invite de commande » -> exécuter en tant qu'administrateur.
- Taper la commande **arp -d**
- Taper **arp -a** pour vérifier le contenu de la table

Q30. Effacer à nouveau la table arp. Effectuer un ping vers le serveur EWTS et vérifier le contenu de la table à nouveau. Que constate-t-on ?

Q31. Relever l'adresse MAC de la carte réseau du serveur.

Adresse MAC du serveur :

Q32. Quel est le constructeur de la carte du serveur ? Cela vous paraît-il cohérent ?

Constructeur de la carte :

Analyse du protocole ARP

Q33. Analyser un ping vers le serveur à l'aide de Wireshark. Combien capture-t-on de trames ARP ? De quels types de trame s'agit-il ? Pour cela :

- Lancer une capture avec Wireshark
- Effectuer un ping vers le serveur.
- Stopper la capture
- Appliquer le filtre **arp** afin de ne conserver que les trames arp

Q34. En observant le champ destination du volet 1 de Wireshark, retrouver à qui est destinée la requête ARP ?

Q35. Quelle est la question posée lors d'une requête ARP (champ « info », volet 1 de Wireshark). Proposer une traduction de cette requête.

Q36. Qui émet la 2^{ème} trame ARP ? Quelle information contient-elle ?

Q37. Vérifier le contenu de la table arp. Que constate-t-on ?

Activité 4 : Synthèse **L'adressage physique**

Chaque carte Ethernet possède une adresse physique unique codée sur ___ octets. C'est l'adresse _____.

Une adresse MAC, par exemple l'adresse suivante 54:42:49:E2:4D:FB, peut être décomposée en deux parties :

Partie Constructeur	Partie hôte

Le protocole _____ permet à un poste de travail de retrouver, à partir de l'adresse _____ :

- l'adresse physique de la carte réseau du destinataire du message si celui-ci appartient au même réseau ou
- l'adresse physique de la carte réseau du premier routeur à traverser si le destinataire n'appartient pas au même réseau.

 **L'adressage IP**

Chaque machine est identifiée sur un réseau IP par une adresse unique (sur ce réseau) : l'adresse IP.

L'adresse IP est composée de ___ octets notés en _____ et séparés par des points (notation décimale pointée).

Ex : 172.31.2.63

L'adresse IP est associée à un _____, de 4 octets également, qui permet de déterminer à quel réseau la machine appartient. En binaire, il est composé d'une suite de bits à 1 puis d'une suite de bits à 0.

L'adresse IP peut être décomposée en deux parties :

- La partie _____
- la partie _____

Le masque de sous-réseau permet de définir la frontière entre ces deux parties.

Par exemple, si on associe le masque 255.255.255.0 à l'adresse IP prise en exemple précédemment,

Q38. Déterminer l'adresse réseau, l'adresse de broadcast ainsi que la plage d'adresses possibles pour ce réseau.

Adresse IP	172.31.2.63
Masque de sous-réseau	255.255.255.0
Adresse réseau	
Adresse de diffusion (broadcast)	
Première adresse de la plage	
Dernière adresse de la plage	

Le nombre de machines adressables sur un réseau donné peut être calculé à l'aide du masque de sous-réseau.

$$n = 2^{\text{nombre_de_bits_à_0_dans_le_masque}} - 2$$

Q39. Déterminer le nombre de machines adressables pour l'exemple précédent

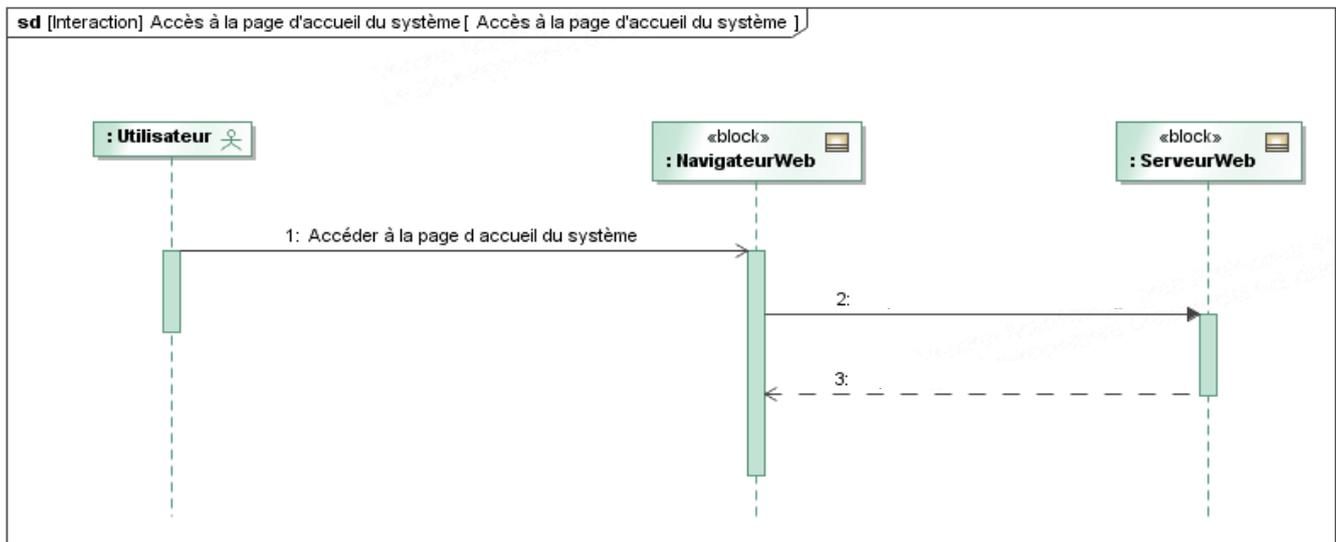
Les adresses IP sont réparties en plusieurs classes.

Classe	Début	Fin	Masque par défaut
Classe ___	0.0.0.0	127.255.255.255	_____.
Classe ___	128.0.0.0	191.255.255.255	_____.
Classe ___	192.0.0.0	223.255.255.255	_____.

Q40. Déterminer la classe à laquelle l'adresse IP de l'exemple précédent appartient

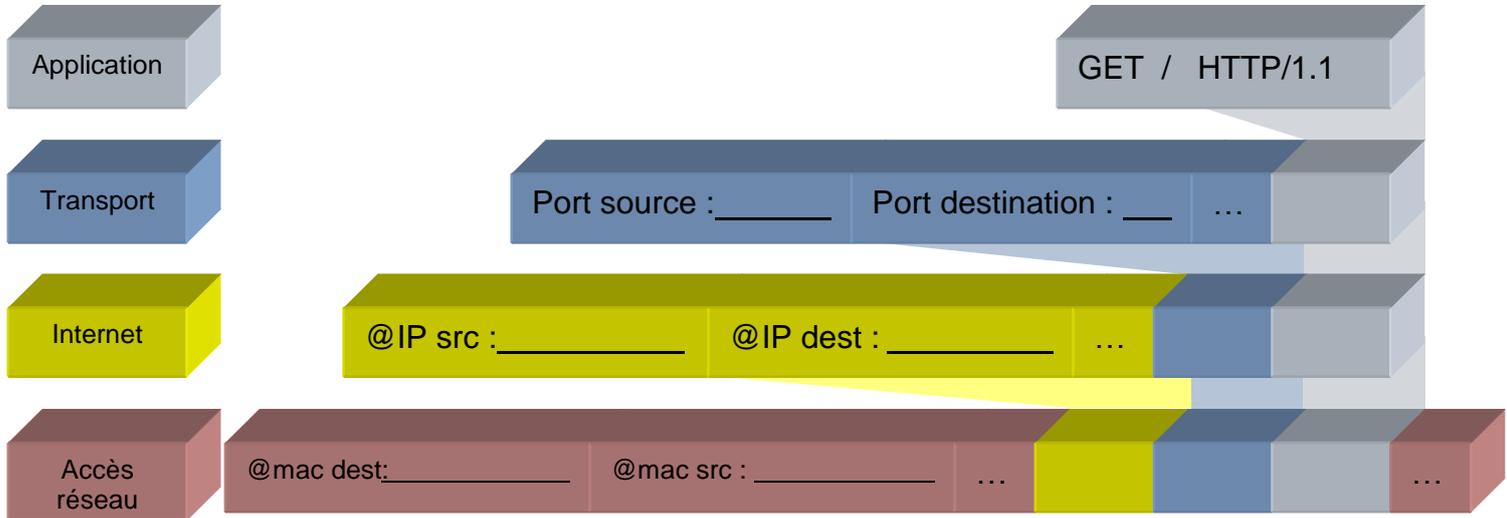
Le modèle Client/Serveur

Q41. Aux vues des activités réalisées précédemment, compléter le diagramme de séquence SysML suivant, montrant la communication entre un client et un serveur HTTP.



 **L'encapsulation des données**

Q42. Compléter la décomposition de la trame transmise par la carte réseau de votre poste de travail lors de la demande de chargement de la page d'accueil du serveur EWTS



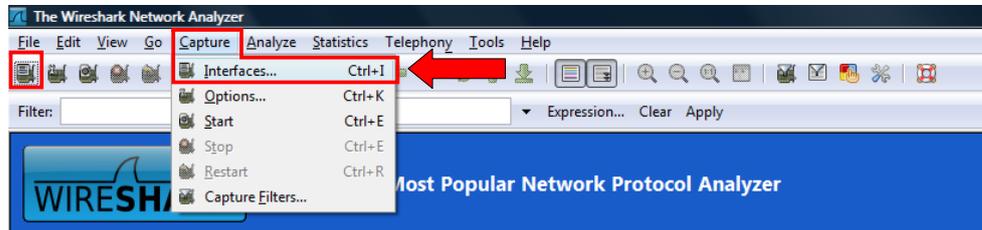
Q43. Compléter le tableau suivant en précisant à quel matériel appartient les adresses MAC source et destination ainsi que les adresses IP source et destination dans la trame.

	valeur	matériel
@ IP source		
@ IP destination		
@ MAC source		
@ MAC destination		

Annexes – Utilisation de Wireshark

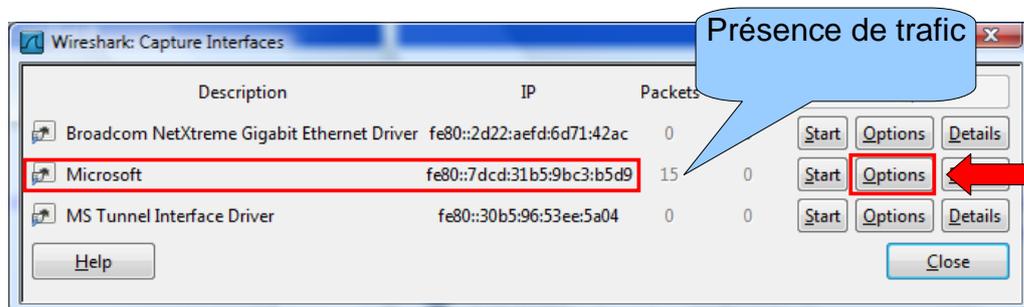
Capture de trames

Avant de lancer une capture, il faut choisir l'interface sur laquelle Wireshark va écouter le trafic.

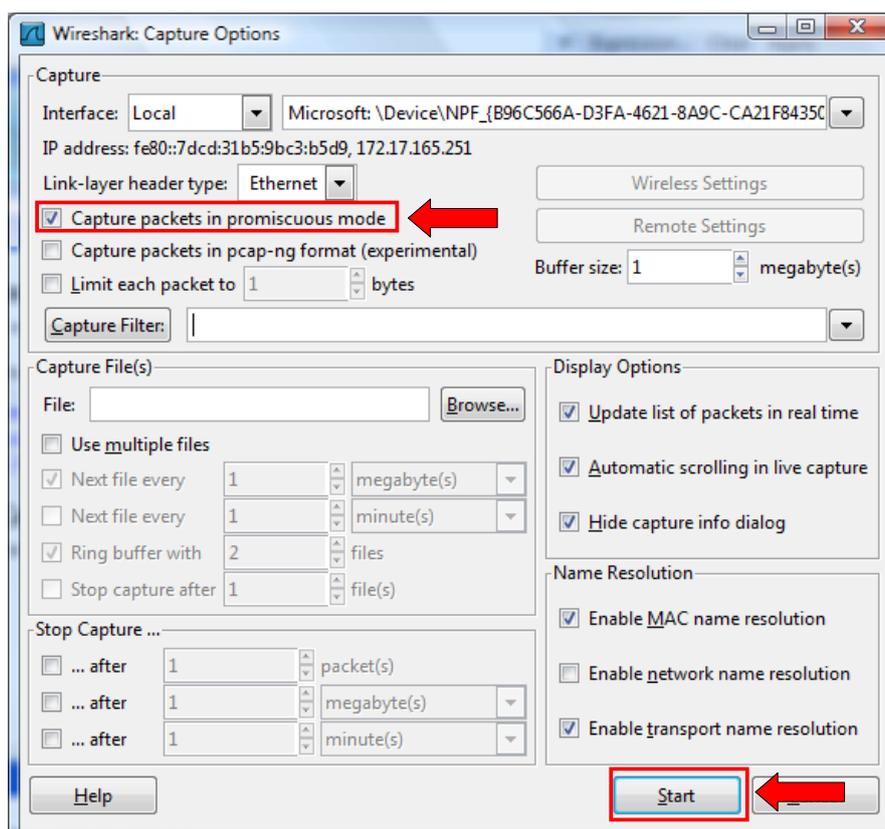


Dans le menu, cliquer sur Capture → Interfaces ou directement sur la première icône.

Dans la nouvelle fenêtre, choisir l'interface souhaitée (généralement celle pour laquelle un trafic apparaît) et cliquer sur Options



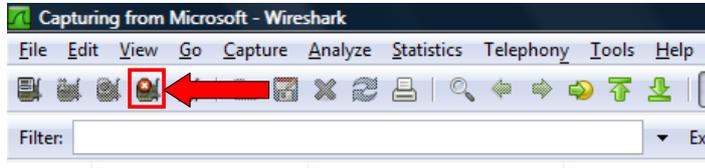
Dans la fenêtre option, vérifier que la case « promiscuous mode » est bien cochée. Cette option



permet de capturer tout le trafic visible par la carte réseau et non pas seulement celui qui lui est directement destiné.

Cliquer alors sur Start pour démarrer la capture.

Effectuer les actions que l'on souhaite analyser. Par exemple, charger la page d'accueil du micro-serveur depuis un navigateur.



Cliquer enfin sur le bouton Stop dans la barre de menu pour arrêter la capture.

Analyse de trame

La fenêtre principale de Wireshark est composée de trois parties:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.10	192.168.0.254	TCP	34246 > http [SYN] Seq=0 win=5840 Len=0 MS...
2	0.001638	192.168.0.254	192.168.0.10	TCP	http > 34246 [SYN, ACK] Seq=0 Ack=1 win=57...
3	0.001703	192.168.0.10	192.168.0.254	TCP	34246 > http [ACK] Seq=1 Ack=1 win=5888 Le...
4	0.002007	192.168.0.10	192.168.0.254	HTTP	GET / HTTP/1.1
5	0.003546	192.168.0.254	192.168.0.10	TCP	http > 34246 [ACK] Seq=1 Ack=393 win=6864 I...
6	1.288756	192.168.0.254	192.168.0.10	TCP	[TCP segment of a reassembled PDU]
7	1.288803	192.168.0.10	192.168.0.254	TCP	34246 > http [ACK] Seq=393 Ack=315 win=691...
8	1.295237	192.168.0.254	192.168.0.10	HTTP	HTTP/1.1 200 OK (text/html)
9	1.295268	192.168.0.10	192.168.0.254	TCP	34246 > http [ACK] Seq=393 Ack=715 win=806...
10	1.430954	192.168.0.10	192.168.0.254	HTTP	GET /loginbar.html HTTP/1.1
11	1.431171	192.168.0.10	192.168.0.254	TCP	34247 > http [SYN] Seq=0 win=5840 Len=0 MS...
12	1.432825	192.168.0.254	192.168.0.10	TCP	http > 34246 [ACK] Seq=715 Ack=830 win=793...
13	1.433685	192.168.0.10	192.168.0.10	TCP	http > 34247 [SYN, ACK] Seq=0 Ack=1 win=57...

Frame 4: 458 bytes on wire (3664 bits), 458 bytes captured (3664 bits)

Ethernet II, Src: CompalIn_4d:b1:16 (00:1b:38:4d:b1:16), Dst: MoxaTech_14:ff:46 (00:90:e8:14:ff:46)

Internet Protocol, Src: 192.168.0.10 (192.168.0.10), Dst: 192.168.0.254 (192.168.0.254)

Transmission Control Protocol, Src Port: 34246 (34246), Dst Port: http (80), Seq: 1, Ack: 1, Len: 392

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Host: 192.168.0.254\r\n

User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; fr; rv:1.9.2.10) Gecko/20100915 ubuntu/9.10 (karmic) Firefox/3.6.10\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: fr,en-us;q=0.7,en;q=0.3\r\n

Accept-Encoding: gzip,deflate\r\n

Accept-Charset: windows-1252,utf-8;q=0.7,*;q=0.7\r\n

Keep-Alive: 115\r\n

Connection: keep-alive\r\n

\r\n

0040 fc 10 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ..GET / HTTP/1.1

0050 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e ..Host: 192.168.

0060 30 2e 32 35 34 0d 0a 55 73 65 72 2d 41 67 65 6e 0.254.U ser-Agen

0070 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (

0080 58 31 31 3b 20 55 3b 20 4c 69 6e 75 78 20 78 38 x11; U; Linux x8

0090 36 5f 36 34 3b 20 66 72 3b 20 72 76 3a 31 2e 39 6_64; fr ; rv:1.9

00a0 2e 32 2e 31 30 29 20 47 65 63 6b 6f 2f 32 30 31 .2.10) G ecko/201

00b0 30 30 39 31 35 20 55 62 75 6e 74 75 2f 39 2e 31 00915 ub untu/9.1

00c0 30 20 28 6b 61 72 6d 69 63 29 20 46 69 72 65 66 0 (karmic) Firef

00d0 6f 78 2f 33 2e 36 2e 31 30 0d 0a 41 63 63 65 70 ox/3.6.1 ..Accep

00e0 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 t: text/ html,app

00f0 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication /xhtml+x

0100 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,appli cation/x

0110 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a 3b 71 3d 30 ml;q=0.9 ,*/*;q=0

0120 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 8 .Acce nt-Langu

1. Cette partie affiche la liste de toutes les trames qui ont été envoyées et reçues entre le début et la fin de la capture. Chaque trame est numérotée et horodatée à la μ s près, la première trame portant le numéro 1 et le temps 0.000000s. On retrouve :

- l'**adresse IP source** = adresse IP de la machine qui a émis la trame, par exemple dans la trame en surbrillance sur la capture précédente, IP source = **192.168.0.10** ; c'est l'adresse IP du poste de travail sur lequel a été effectuée la capture.
- l'**adresse IP destination** = adresse IP de la machine à qui était destinée la trame, dans l'exemple : **192.168.0.254** ; il s'agit de l'adresse IP du micro-serveur.
- le **protocole de communication de plus au niveau** utilisé pour la communication. Dans l'exemple il s'agit du protocole **HTTP**.
- Un **résumé du contenu du message** transmis. Ici, on retrouve le détail de la requête HTTP : **GET / HTTP/1.1**. Cette requête signifie que l'on désire obtenir (GET) la page par défaut du serveur web auquel on s'adresse (/) en utilisant la version 1.1 du protocole HTTP (HTTP/1.1)

2. Cette partie de la fenêtre montre le détail de la trame qui a été sélectionnée dans le volet.

- la première ligne montre l'intégralité de la trame
- les lignes suivantes montrent la décomposition de cette trame suivant les couches successives du modèle TCP/IP, chaque couche ajoutant son lot d'informations.

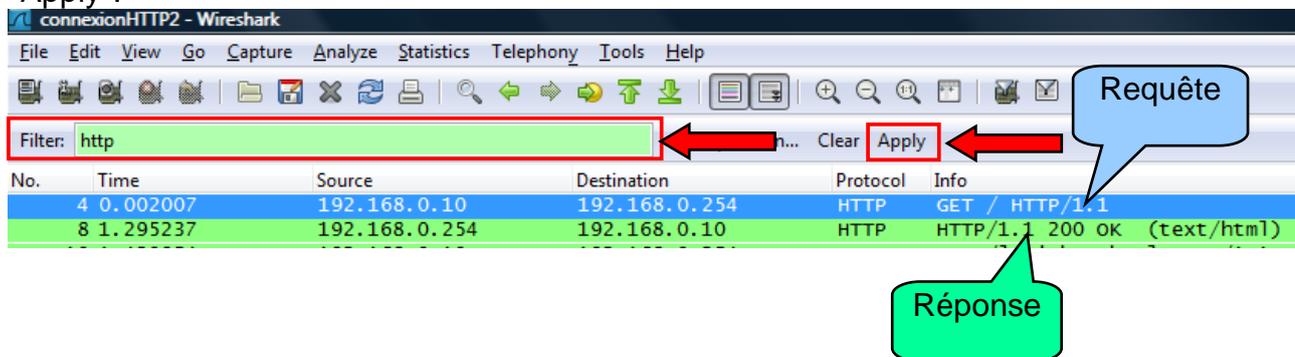
***Rque :** Dans l'exemple, on retrouve les informations de niveau application (la requête HTTP). On pourrait retrouver notamment le code HTML contenu dans la réponse du serveur. On retrouve également les informations relatives à TCP (notamment les ports source et destination), celles ajoutées par la couche IP (adresses IP source et destination) et enfin les informations de la couche accès au réseau, ici Ethernet (adresses MAC source et destination).*

3. Cette partie affiche directement les octets qui composent la trame ainsi que leur représentation au format ASCII

Astuces pour l'utilisation de Wireshark

Astuce 1 : Une grande quantité de trames de différentes natures peuvent transiter sur le réseau lors de la capture. Afin d'isoler les trames qui nous intéressent spécialement, on peut appliquer des filtres.

Par exemple pour conserver uniquement le dialogue HTTP entre le poste de travail et le micro-serveur, il suffit de saisir **http** dans le champ "filter" en haut du 1er volet et de cliquer sur "Apply".



***Rque :** De la même façon, on pourrait isoler les ping (requêtes et réponses) entre deux machines en saisissant **icmp** dans le champ "filter" qui correspond au nom du protocole utilisé pour l'envoi des ping.*

Astuce 2 : En effectuant un clic droit sur un trame dans le volet 1 puis "Follow TCP Stream", on peut suivre l'intégralité du dialogue entre les deux machines au niveau de la couche application. Ci-dessous en rouge la requête HTTP effectuée par le poste de travail et en bleu la réponse du micro-serveur.

The screenshot shows a 'Follow TCP Stream' window with the following content:

```
Stream Content
GET / HTTP/1.1
Host: 192.168.0.254
User-Agent: Mozilla/5.0 (X11; U; Linux x86_64; fr; rv:1.9.2.10) Gecko/20100915 Ubuntu/9.10 (karmic)
Firefox/3.6.10
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: windows-1252,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 19 Oct 2010 15:21:54 GMT
Server: Apache/2.2.8 (Unix) mod_ssl/2.2.8 OpenSSL/0.9.8i
Last-Modified: Thu, 07 Jan 2010 16:45:50 GMT
ETag: "c6-190-47c95cdb4eb80"
Accept-Ranges: bytes
Content-Length: 400
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!doctype HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN" "http://www.w3.org/TR/html4/frameset.dtd">
<html>
<head>
<title>Rugged Micro Server MSD10</title>
</head>
<frameset frameborder="NO" border="0" framespacing="0" ROWS="175,*">
  <frame name="menu" scrolling="NO" noresize src="/loginbar.html">
  <frame name="main" src="/login.html">
</frameset>
<noframes>
<body>
</body>
</noframes>
</html>
```

Callouts in the image:

- Requête HTTP du client** (red callout pointing to the GET request)
- Réponse du serveur** (blue callout pointing to the HTTP 200 OK response)
- Code HTML de la page retournée** (blue callout pointing to the HTML body content)