université de BORDEAUX

Collège Sciences et technologies

Année Universitaire	2015-2016	***Période***	Session de Printemps
Code Etape	MIAGE L3	***Code UE***	J1IN6026
Nom de l'Epreuve	Utilisation des Réseaux		
Date / Heure	24/03/2016 à 10h00	***Durée***	1h00
Documents	Non autorisés	***Calculatrice***	Oui
Nombre de pages	4	***Enseignant***	A. Esnard

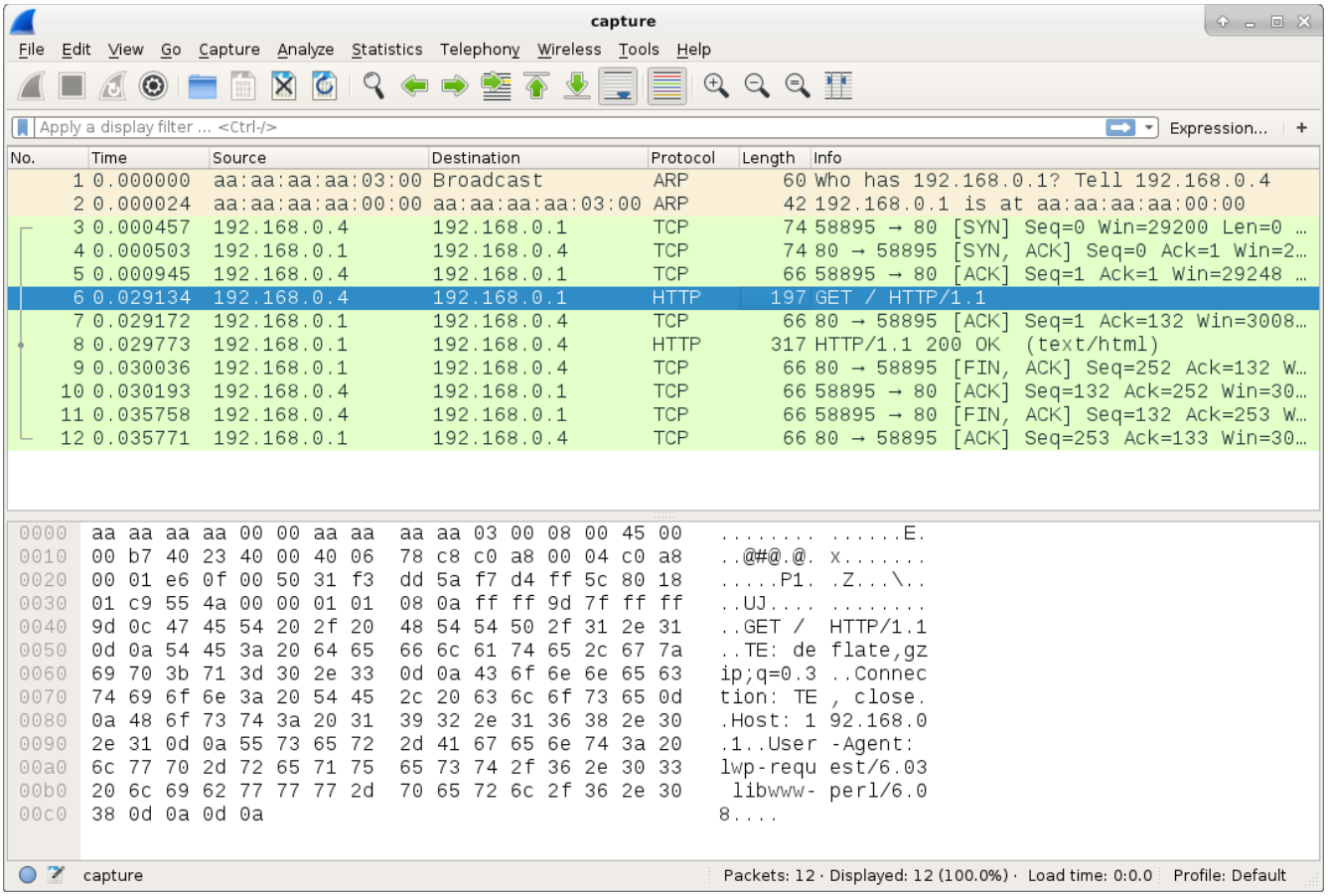
Nota Bene : Le barème est donné à titre indicatif. Vous disposez d'annexes pour vous aider.

Ex 1 (Questions Préliminaires, 10 pt)

1. Soit le réseau 192.168.1.128/26. Combien de machines peut-on numéroter dans un tel réseau ? Donner le masque. Donner la plage d'adresses IP pour les machines de ce réseau. **(3 pt)**
2. Soit le polynôme générateur : $x^3 + x + 1$. On souhaite transmettre le message binaire « 1111 0000 ». Calculez le bloc de contrôle d'erreur CRC en prenant soin de détailler les calculs. **(3 pt)**
3. Un LAN Ethernet 192.168.0.0/24 est relié à Internet par une passerelle G qui dispose d'une adresse IP publique 76.125.206.94 sur eth0 et d'une adresse privée 192.168.0.254 sur eth1. Vous branchez votre portable P dans ce LAN.
   - Donnez la liste des commandes nécessaires pour que la machine P accède à Internet. A vous de choisir son adresse IP. **(2 pt)**
   - On souhaite maintenant configurer un firewall sur G (politique par défaut à DROP) afin de permettre à la machine P de consulter uniquement des pages web (TCP, port 80). Donnez la liste des commandes nécessaires. **(2 pt)**

Ex 2 (Analyse de Trame, 10 pt)

On considère la capture *tcpdump* de trames Ethernet suivante, visualisé grâce à l'outil *Wireshark* :

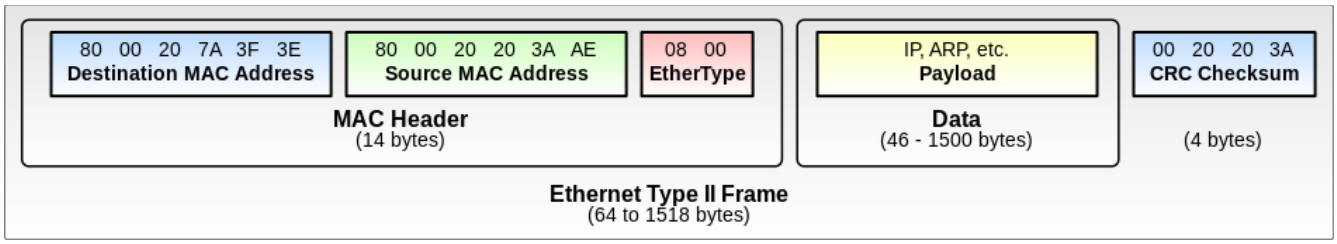


1. Décrire précisément le rôle des trames n° 1 et 2 ?
2. Quel est le rôles des trames n° 3 à 5 ? De même, quel est le rôle des trames n° 9 à 12 ?
3. A quoi correspond selon vous l'échange des trames n° 6 et 8 ?

On se concentre maintenant sur le détail de la trame n° 6 affichée ci-dessus au format hexedécimal. Chaque ligne représente 16 octets. Pour vous aider à répondre aux questions suivantes, vous trouverez en annexe une description des en-têtes Ethernet, IP et TCP.

4. Quel est l'adresse MAC source et destination ? Quel est la valeur de *EtherType* ? Que représente selon vous cette valeur ?
5. Dans le paquet IP, quelle est la valeur du champs IHL (Internet Header Length) ? Ce nombre représente la longueur de l'en-tête du paquet IP, comptée en mots de 32 bits. En déduire la taille en octets de cette en-tête ?
6. Que trouve-t-on immédiatement après l'en-tête IP ? Que représente les 4 premiers octets ? Décodez ces valeurs ? Que pouvez-vous en déduire ?
7. Que représente selon vous les données de la trame à partir de l'adresse 0x0043, débutant par les valeurs “47 45 54 ...” dont vous avez la traduction en caractère ASCII dans la colonne de droite. Justifiez.

Annexes I



IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Annexes II

Memento Routage

- Activer le routage sur une machine (ip forward) : echo 1 > /proc/sys/net/ipv4/ip_forward
- Afficher la table de routage : route -n
- Définir une route par défaut : route add default gw <@gateway>
- Ajouter une route vers un réseau : route add -net <@network> netmask <mask> gw <@gateway>
- Ajouter une route vers une machine particulière : route add -host <@host> gw <@gateway>
- Pour supprimer une règle, il faut taper la commande route del <…> avec exactement les mêmes arguments que pour la commande add.

Memento Firewall

Voici quelques notes concernant l'utilisation d'iptables pour configurer un firewall. La configuration du firewall se base sur la table “filter” et est subdivisée en 3 chaînes (notée <CHAIN>) : INPUT : tout ce qui rentre dans la machine ; OUTPUT : tout ce qui sort dans la machine ; FORWARD : tout ce qui traverse la machine (i.e. lors du routage).

- Pour afficher les règles de la table filter : iptables -t filter -L
- Pour effacer toutes les règles ajoutées : iptables -t filter -F
- Pour chaque règle que l'on ajoute, trois actions sont possibles (notée <ACTION>) :
  - ACCEPT : on accepte ;
  - REJECT : on rejette poliment (réponse d'erreur envoyé à l'émetteur) ;
  - DROP : on jette à la poubelle (pas de réponse d'erreur).
- Pour modifier la politique par défaut du firewall : iptables -t filter -P <CHAIN> <ACTION>
- Pour ajouter une nouvelle règle à une chaîne du firewall (attention à l'ordre des règles) : iptables -t filter -A <CHAIN> <SRC> <DST> <...> -j <ACTION>
  - avec <SRC> des indications sur la provenance des paquets IP, comme par exemple ”-i eth0” ou ”-s 192.168.0.0/24” ou encore ”-s 0/0” ;
  - avec <DST> des indications sur la destination des paquets IP, comme par exemple : ”-o eth1” ou ”-d 147.210.0.0/24” ;
  - avec <…> des infos complémentaires sur par exemple la nature du protocole ”-p icmp” ou ”-p tcp”, avec éventuellement des precisions spécifiques à ces protocoles (”-dport 80” pour TCP) ou encore sur l'état ”-m state –state NEW”, …

Correction

Ex 1 (Questions Préliminaires, 10 pt)

1. Soit le réseau 192.168.1.128/26. Combien de machines peut-on numéroter dans un tel réseau ? Donner le masque. Donner la plage d'adresses IP pour les machines de ce réseau. **(3 pt)**

   Un masque /26 désigne des plages de $2^{(32-26)} = 64$ adresses pour ce réseau, et donc de 64-2=62 machines. Masque : 255.255.255.192. La plage d'adresse IP de ce réseau est donc:192.168.1.128-192.168.1.192.

2. Soit le polynôme générateur : $x^3 + x + 1$. On souhaite transmettre le message binaire « 1111 0000 ». Calculez le bloc de contrôle d'erreur CRC en prenant soin de détailler les calculs. **(3 pt)**

   $P(x) = x^7 + x^6 + x^5 + x^4$
   $P(x).x^3 = x^{10} + x^9 + x^8 + x^7$
   On caclule la division de $P(x).x^3$ par $G(x) = x^3 + x + 1$. On trouve un reste $R(x) = x^2$ et donc la clef CRC sur 3 bits est « 100 ».

3. Un LAN Ethernet 192.168.0.0/24 est relié à Internet par une passerelle G qui dispose d'une adresse IP publique 76.125.206.94 sur eth0 et d'une adresse privée 192.168.0.254 sur eth1. Vous branchez votre portable P dans ce LAN.

   - Donnez la liste des commandes nécessaires pour que la machine P accède à Internet. A vous de choisir son adresse IP. **(2 pt)**

     ```
     P$ ifconfig eth0 192.168.0.1/24          # en supposant que @P = 192.168.0.1
     P$ route add default gw 192.168.0.254
     ```

   - On souhaite maintenant configurer un firewall sur G (politique par défaut à DROP) afin de permettre à la machine P de consulter uniquement des pages web (TCP, port 80). Donnez la liste des commandes nécessaires. **(2 pt)**

     ```
     G$ iptables -P INPUT DROP
     G$ iptables -P OUTPUT DROP
     G$ iptables -P FORWARD DROP
     G$ iptables -A FORWARD -s 192.168.0.1 -p tcp --dport 80 -A ACCEPT
     G$ iptables -A FORWARD -d 192.168.0.1 -p tcp --sport 80 -m state --state ESTABLISHED -A ACCEPT
     ```

Ex 2 (Analyse de Trame, 10 pt)

Quelques éléments de corrections rapides...

1. Décrire précisément le rôle des trames n° 1 et 2 ?
   Trame n° 1 : Dans un LAN Ethernet, la machine 192.168.0.4 effectue une requête ARP en Broadcast pour trouver l'adresse MAC de 192.168.0.1.
   Trame n° 2 : Réponse ARP, la machine 192.168.0.1 envoie son adresse MAC à 192.168.0.4.

2. Quel est le rôles des trames n° 3 à 5 ? De même, quel est le rôle des trames n° 9 à 12 ?

   Trame n° 3 à 5 : Ouverture d'une connexion TCP/IP de 192.168.0.4 (client) vers 192.168.0.1 (serveur sur port 80). On voit la traditionnelle poignée de main TCP/IP en trois temps :SYN,

puis SYN-ACK, puis ACK.
Trame n° 9 à 12 : Fermeture de la connexion TCP/IP (flag FIN) à la demande du serveur (192.168.0.1).

3. A quoi correspond selon vous l'échange des trames n° 6 et 8 ?

   Trame n° 6 : Il s'agit d'une requête HTTP « GET / HTTP/1.1 » du client web (192.168.0.4) vers le serveur web (192.168.0.1).
   Trame n° 8 : Réponse du serveur web de la page web demandée (« / » est la page d'accueil) sous format text/html.

On se concentre maintenant sur le détail de la trame n° 6 affichée ci-dessus au format hexedécimal. Chaque ligne représente 16 octets. Pour vous aider à répondre aux questions suivantes, vous trouverez en annexe une description des en-têtes Ethernet, IP et TCP.

```
0000   aa aa aa aa 00 00 aa aa aa aa 03 00 08 00 45 00   ..............E.
0010   00 b7 40 23 40 00 40 06 78 c8 c0 a8 00 04 c0 a8   ..@#@.@.x.......
0020   00 01 e6 0f 00 50 31 f3 dd 5a f7 d4 ff 5c 80 18   .....P1..Z...\..
0030   01 c9 55 4a 00 00 01 01 08 0a ff ff 9d 7f ff ff   ..UJ............
0040   9d 0c 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31   ..GET / HTTP/1.1
0050   0d 0a 54 45 3a 20 64 65 66 6c 61 74 65 2c 67 7a   ..TE: deflate,gz
0060   69 70 3b 71 3d 30 2e 33 0d 0a 43 6f 6e 6e 65 63   ip;q=0.3..Connec
0070   74 69 6f 6e 3a 20 54 45 2c 20 63 6c 6f 73 65 0d   tion: TE, close.
0080   0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 30   .Host: 192.168.0
0090   2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20   .1..User-Agent:
00a0   6c 77 70 2d 72 65 71 75 65 73 74 2f 36 2e 30 33   lwp-request/6.03
00b0   20 6c 69 62 77 77 77 2d 70 65 72 6c 2f 36 2e 30    libwww-perl/6.0
00c0   38 0d 0a 0d 0a                                    8....
```

Headers : Ethernet = bleu, IP = jaune, TCP = vert. Puis le reste en blanc, la requête HTTP.

4. Quel est l'adresse MAC source et destination ? Quel est la valeur de *EtherType* ? Que représente selon vous cette valeur ?

   Analyse du header Ethernet en bleu ci-dessus.
   @MAC destination : aa aa aa aa 00 00
   @MAC source : aa aa aa aa 03 00
   EtherType : 08 00 (La trame Ethernet contient un paquet IP.)

5. Dans le paquet IP, quelle est la valeur du champs IHL (Internet Header Length) ? Ce nombre représente la longueur de l'en-tête du paquet IP, comptée en mots de 32 bits. En déduire la taille en octets de cette en-tête ?

   IHL vaut 5 (dans le 1er octet, deuxième caractère hexa), ce qui indique une longueur de 5x4=20 octets pour le header IP (en jaune ci-dessus).

6. Que trouve-t-on immédiatement après l'en-tête IP ? Que représente les 4 premiers octets ? Décodez ces valeurs ? Que pouvez-vous en déduire ?

   On trouve le header du segment TCP. Les 4 premiers octets représentent le port source (2 octets) et le port destination du protocole TCP qui on respectivement les valeurs 58895 et 80 en décimal.

   On peut en déduire que l'on discute en TCP/IP vers le port 80 de la machine 192.168.0.4, qui joue a priori le rôle d'un serveur web.

7. Que représente selon vous les données de la trame à partir de l'adresse 0x0043, débutant par les valeurs “47 45 54 ...” dont vous avez la traduction en caractère ASCII dans la colonne de droite. Justifiez. Il s'agit des données de la requête HTTP « GET / HTTP/1.1 ». (...)