1 **Examen Réparti 1 : ARES 2011-2012** 1

Durée totale: *2h00*
Autorisé: *Une feuille A4 manuscrite*
Non autorisés: *Autres documents, calculatrices, téléphones portables, PDA, etc.*

Voici **3** feuilles recto/verso, contenant le sujet et les champs de réponse, que vous devrez **exclusivement** nous rendre en fin d'épreuve. Pour garantir l'anonymat, un numéro aléatoire vous sera fourni et devra être collé sur **chacune** des feuilles du sujet et sur la feuille d'émargement. Vous devez noter vos réponses directement sur ce sujet dans les cadres correspondants.

1 Couche application *(6 points)*

Vous souhaitez accéder à une page Web identifiée par l'URL suivante : `http://www.serveur_web_de_Bob.fr/Bob.html`

Le contenu de cette page html est le suivant :

```
<HTML>
<HEAD>
      <TITLE> Page perso de Bob !!! </TITLE>
</HEAD>
<BODY>
<P> Voici quelques photos ! </P>
<IMG SRC= "image1.gif" >
<IMG SRC= "im2.gif" >
<IMG SRC= "http://www.ma_ville.fr/picture.jpg" >
</BODY>
</HTML>
```

Afin de visiter cette page, vous allumez votre machine, tous les caches impliqués sont vides. La version du protocole HTTP utilisée est 1.1 avec *pipelining*. Chaque image de la page de Bob est de très petite taille et tient dans un paquet. Dans le cas où des requêtes DNS sont nécessaires dans cet exercice, on considère que le serveur DNS local utilisé contacte en moyenne 3 serveurs DNS de manière itérative pour obtenir une réponse.

1. **Représentez à l'aide de schémas toutes les étapes nécessaires** (aux niveaux 4 et 5 de la pile TCP/IP) pour afficher la page Web complète, en indiquant les événements successifs, ainsi que ceux qui se produisent (éventuellement) en parallèle.

2. Donnez une formule littérale du délai correspondant.

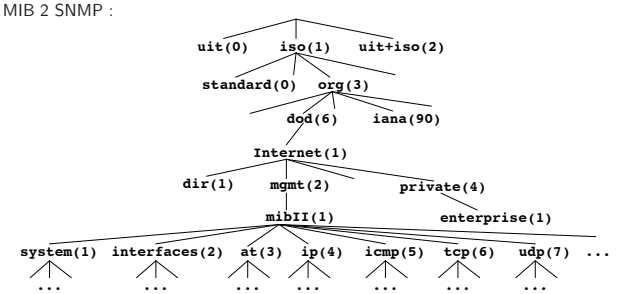
3. Bob est administrateur de son réseau et souhaite visualiser des informations SNMP relatives au système de son serveur Web. Dans un terminal, il lance la commande suivante :

   `snmpwalk -c public serveur_web_de_Bob.fr system`

   En vous aidant de la structure de la MIB fournie ci-dessous, quels sont les attributs SNMP dont les valeurs vont s'afficher sur l'écran de Bob ?

4. Quelle est la séquence de messages SNMP (requêtes ET réponses) générés par la commande tapée par Bob ?

Structure de la MIB 2 SNMP :



Détail des informations du groupe `system` :

(1)	`sysDescr`	description du device
(2)	`sysObjectID`	identité de l'agent
(3)	`sysUpTime`	depuis combien de temps l'agent est démarré
(4)	`sysContact`	nom de la personne à contacter
(5)	`sysName`	nom du device
(6)	`sysLocation`	localisation physique du device
(7)	`sysServices`	services offerts par le device
...	...	...

2

Examen Réparti 1 : ARES 2011-2012

Durée totale: *2h00*
Autorisé: *Une feuille A4 manuscrite*
Non autorisés: *Autres documents, calculatrices, téléphones portables, PDA, etc.*

2

Voici **3** feuilles recto/verso, contenant le sujet et les champs de réponse, que vous devrez **exclusivement** nous rendre en fin d'épreuve. Pour garantir l'anonymat, un numéro aléatoire vous sera fourni et devra être collé sur **chacune** des feuilles du sujet et sur la feuille d'émargement. Vous devez noter vos réponses directement sur ce sujet dans les cadres correspondants.

2 Transport *(7 points)*

Voici la sortie textuelle d'une capture réalisée avec l'analyseur `tcpdump` (similaire à `wireshark`) sur une interface réseau :

```
 1  10.1.1.1.59590 > 10.1.2.1.53:  59155+ A? serveur.etu1.plateforme.lan. (45)
 2  10.1.2.1.53 > 10.1.1.1.59590:  59155* 1/1/1 A 10.1.2.1 (94)
 3  10.1.1.1.55872 > 10.1.2.1.21: S 809225706:809225706(0) win 5840 <mss 1460,sackOK,timestamp 35153644 0,nop,
                                                                    wscale 6>
 4  10.1.2.1.21 > 10.1.1.1.55872: S 3176008790:3176008790(0) ack 809225707 win 5792 <mss 1460,sackOK,
                                                                    timestamp 70589315 35153644,nop,wscale 6>
 5  10.1.1.1.55872 > 10.1.2.1.21: . ack 1 win 92 <nop,nop,timestamp 35153644 70589315>
 6  10.1.2.1.21 > 10.1.1.1.55872: P 1:66(65) ack 1 win 91 <nop,nop,timestamp 70589316 35153644>
 7  10.1.1.1.55872 > 10.1.2.1.21: . ack 66 win 92 <nop,nop,timestamp 35153646 70589316>
 8  10.1.1.1.55872 > 10.1.2.1.21: P 1:15(14) ack 66 win 92 <nop,nop,timestamp 35155052 70589316>
 9  10.1.2.1.21 > 10.1.1.1.55872: . ack 15 win 91 <nop,nop,timestamp 70590722 35155052>
10  10.1.2.1.21 > 10.1.1.1.55872: P 66:102(36) ack 15 win 91 <nop,nop,timestamp 70590723 35155052>
11  10.1.1.1.55872 > 10.1.2.1.21: . ack 102 win 92 <nop,nop,timestamp 35155052 70590723>
12  10.1.1.1.55872 > 10.1.2.1.21: P 15:25(10) ack 102 win 92 <nop,nop,timestamp 35155572 70590723>
13  10.1.2.1.21 > 10.1.1.1.55872: P 102:175(73) ack 25 win 91 <nop,nop,timestamp 70591243 35155572>
14  10.1.1.1.55872 > 10.1.2.1.21: . ack 175 win 92 <nop,nop,timestamp 35155572 70591243>
15  10.1.2.1.21 > 10.1.1.1.55872: P 175:532(357) ack 25 win 91 <nop,nop,timestamp 70591243 35155572>
16  10.1.1.1.55872 > 10.1.2.1.21: . ack 532 win 108 <nop,nop,timestamp 35155572 70591243>
17  10.1.1.1.55872 > 10.1.2.1.21: P 25:31(6) ack 532 win 108 <nop,nop,timestamp 35155572 70591243>
18  10.1.2.1.21 > 10.1.1.1.55872: P 532:559(27) ack 31 win 91 <nop,nop,timestamp 70591243 35155572>
19  10.1.1.1.55872 > 10.1.2.1.21: . ack 559 win 108 <nop,nop,timestamp 35155583 70591243>
20  10.1.1.1.55872 > 10.1.2.1.21: P 31:39(8) ack 559 win 108 <nop,nop,timestamp 35159724 70591243>
21  10.1.2.1.21 > 10.1.1.1.55872: P 559:579(20) ack 39 win 91 <nop,nop,timestamp 70595395 35159724>
22  10.1.1.1.55872 > 10.1.2.1.21: . ack 579 win 108 <nop,nop,timestamp 35159724 70595395>
23  10.1.1.1.55872 > 10.1.2.1.21: P 39:61(22) ack 579 win 108 <nop,nop,timestamp 35159724 70595395>
24  10.1.2.1.21 > 10.1.1.1.55872: P 579:609(30) ack 61 win 91 <nop,nop,timestamp 70595395 35159724>
25  10.1.1.1.55872 > 10.1.2.1.21: P 61:76(15) ack 609 win 108 <nop,nop,timestamp 35159724 70595395>
26  10.1.2.1.20 > 10.1.1.1.58173: S 3567938350:3567938350(0) win 5840 <mss 1460,sackOK,timestamp 70595395 0,nop,
                                                                    wscale 6>
27  10.1.1.1.58173 > 10.1.2.1.20: S 1175404437:1175404437(0) ack 3567938351 win 5792 <mss 1460,sackOK,
                                                                    timestamp 35159724 70595395,nop,wscale 6>
28  10.1.2.1.20 > 10.1.1.1.58173: . ack 1 win 92 <nop,nop,timestamp 70595395 35159724>
29  10.1.2.1.21 > 10.1.1.1.55872: P 609:677(68) ack 76 win 91 <nop,nop,timestamp 70595395 35159724>
30  10.1.2.1.20 > 10.1.1.1.58173: P 1:24(23) ack 1 win 92 <nop,nop,timestamp 70595395 35159724>
31  10.1.2.1.20 > 10.1.1.1.58173: F 24:24(0) ack 1 win 92 <nop,nop,timestamp 70595395 35159724>
32  10.1.1.1.58173 > 10.1.2.1.20: . ack 24 win 91 <nop,nop,timestamp 35159725 70595395>
33  10.1.1.1.58173 > 10.1.2.1.20: F 1:1(0) ack 25 win 91 <nop,nop,timestamp 35159725 70595395>
34  10.1.2.1.20 > 10.1.1.1.58173: . ack 2 win 92 <nop,nop,timestamp 70595396 35159725>
35  10.1.1.1.55872 > 10.1.2.1.21: . ack 677 win 108 <nop,nop,timestamp 35159735 70595395>
36  10.1.2.1.21 > 10.1.1.1.55872: P 677:701(24) ack 76 win 91 <nop,nop,timestamp 70595405 35159735>
37  10.1.1.1.55872 > 10.1.2.1.21: . ack 701 win 108 <nop,nop,timestamp 35159735 70595405>
38  10.1.1.1.55872 > 10.1.2.1.21: P 76:82(6) ack 701 win 108 <nop,nop,timestamp 35160528 70595405>
39  10.1.2.1.21 > 10.1.1.1.55872: P 701:715(14) ack 82 win 91 <nop,nop,timestamp 70596199 35160528>
40  10.1.2.1.21 > 10.1.1.1.55872: F 715:715(0) ack 82 win 91 <nop,nop,timestamp 70596199 35160528>
41  10.1.1.1.55872 > 10.1.2.1.21: . ack 715 win 108 <nop,nop,timestamp 35160528 70596199>
42  10.1.1.1.55872 > 10.1.2.1.21: F 82:82(0) ack 715 win 108 <nop,nop,timestamp 35160528 70596199>
43  10.1.1.1.55872 > 10.1.2.1.21: . ack 716 win 108 <nop,nop,timestamp 35160528 70596199>
44  10.1.2.1.21 > 10.1.1.1.55872: . ack 83 win 91 <nop,nop,timestamp 70596199 35160528>
```


Il est conseillé de tracer au préalable un chronogramme des échanges (sur une feuille de brouillon à ne pas rendre).

1. Quels sont les protocoles applicatifs impliqués (justifiez) ?
2. Quels sont les protocoles de transport observés (justifiez) ?
3. Sur quel poste de travail de l'ARI cette trace a-t-elle été obtenue ? Donner 2 justifications.
4. Combien de connexions TCP figurent sur la trace et quels sont les numéros de ports utilisés (justifiez) ?
5. Quels sont les valeurs des ISN (valeurs réellement échangées et non pas relatives affichées par l'analyseur) ?
6. La trace fait apparaître des valeurs de fenêtre relativement faibles (par exemple, une valeur de 92 dans la trame 5). Est-ce normal ?
7. Combien de commandes du protocole applicatif ont été envoyées ? Quelles sont-elles et à quoi servent-elles ?
8. Combien d'octets d'informations utiles ont été envoyés, et de qui à qui ?
9. Quel est le but de cet échange ?

3

Examen Réparti 1 : ARES 2011-2012

Durée totale: *2h00*
Autorisé: *Une feuille A4 manuscrite*
Non autorisés: *Autres documents, calculatrices, téléphones portables, PDA, etc.*

3

Voici **3** feuilles recto/verso, contenant le sujet et les champs de réponse, que vous devrez **exclusivement** nous rendre en fin d'épreuve. Pour garantir l'anonymat, un numéro aléatoire vous sera fourni et devra être collé sur **chacune** des feuilles du sujet et sur la feuille d'émargement. Vous devez noter vos réponses directement sur ce sujet dans les cadres correspondants.

3 Analyse protocolaire *(7 points)*

1. Voici la trace d'une première trame Ethernet présentée en 3 colonnes de manière identique à celles étudiées en TD+TME. Délimitez et identifiez soigneusement les champs de tous les niveaux protocolaires (utilisez si possible une couleur par protocole). Vous disposez pour cela de l'annexe page 7.

```
0000  00 09 5b 95 9f 3a 08 00 46 b1 49 5e 08 00 45 00   ..[..:..F.I^..E.
0010  00 43 00 00 40 00 40 11 b9 64 0a 21 b6 05 0a 21   .C..@.@..d.!...!
0020  b6 fe 80 05 00 35 00 2f b4 99 bd 25 01 00 00 01   .....5./...%....
0030  00 00 00 00 00 00 03 77 77 77 0d 61 6d 62 61 66   .......www.ambaf
0040  72 61 6e 63 65 2d 76 6e 03 6f 72 67 00 00 01 00   rance-vn.org....
0050  01
```

2. Voici une seconde trame Ethernet. Réalisez la même analyse.

```
0000  08 00 46 b1 49 5e 00 09 5b 95 9f 3a 08 00 45 00   ..F.I^..[..:..E.
0010  00 61 0c c1 00 00 40 11 ec 85 0a 21 b6 fe 0a 21   .a....@....!...!
0020  b6 05 00 35 80 05 00 4d 50 d8 bd 25 81 80 00 01   ...5...MP..%....
0030  00 02 00 00 00 00 03 77 77 77 0d 61 6d 62 61 66   .......www.ambaf
0040  72 61 6e 63 65 2d 76 6e 03 6f 72 67 00 00 01 00   rance-vn.org....
0050  01 c0 0c 00 05 00 01 00 00 38 40 00 02 c0 10 c0   .........8@.....
0060  10 00 01 00 01 00 00 38 40 00 04 4a 34 07 f2      .......8@..J4..
```


3. Quelles sont les adresses IP utilisées ?

4. Vérifiez que les traces présentent l'intégralité des octets des trames émisent sur le réseau. Justifiez votre réponse

5. A quoi sert le champ d'identification des messages applicatifs ?

6. Quelles informations le protocole de la couche application permet-il de récupérer lors de l'échange des deux trames précédentes ?

7. Quelle action applicative a pus déclencher cet échange ?

Annexe

Structure de la trame Ethernet

Trame présentée sans préambule ni CRC :

```
+--48-bits--+--48-bits--+16b-+-  -  -  -  -+
|  adresse  |  adresse  |type|   données    |
|destination|   source  |    |              |
+-----------+-----------+----+-  -  -  -  -+

Quelques types : 0x0800 = DoD Internet (IPv4)
                 0x0806 = ARP
```

Structure du paquet IPv4

```
<-----------------32bits----------------------->
<-4b->      <--8bits--->  <--------16bits-------->
+-----+-----+-----------+-----------------------+
| Ver | IHL | TOS       | Longueur totale       |
+-----+-----+-----------+--+--------------------+
| Identificateur        |Fl| FO                 |
+-----------+-----------+--+--------------------+
| TTL       | Protocole | Somme de ctrl (entête)|
+-----------+-----------+-----------------------+
| Adresse Source                                |
+-----------------------------------------------+
| Adresse Destination                           |
+-----------------------------------------------+
...     Options
+-----------------------------------------------+
...     Données
+-----------------------------------------------+

Ver = Version d'IP
IHL = Longueur de l'en-tête IP (en mots de 32 bits)
TOS = Type de service
Longueur totale du paquet IP (en octets)
Fl (3 premiers bits) = indicateurs pour la fragmentation
   (Reservé|Ne pas fragmenter|Fragment suivant existe)
FO (13 bits suivants) = Décalage du fragment
 * valeur a multiplier par 8 octets
TTL = Durée de vie restante
Quelques protocoles transportés :
        1 = ICMP                11 = BLUP
        6 = TCP                 17 = UDP
```

Structure de segment TCP

```
<-----------------32bits----------------------->
<-4b->         <-6bits-><--------16bits-------->
+-----------------------+-----------------------+
| Port Source           |  Port Destination     |
+-----------------------+-----------------------+
| Numéro de Séquence                            |
+-----------------------------------------------+
| Numéro d'Acquittement                         |
+-----+-------+---------+-----------------------+
| THL |       |  Flag   |  Taille Fenêtre       |
+-----+-------+---------+-----------------------+
| Somme de ctrl (message)  Pointeur d'Urgence   |
+-----------------------+-----------------------+
...      Options
+-----------------------------------------------+
...      Données
+-----------------------------------------------+

THL = Longueur de l'entête TCP sur 4 bits (*32bits)
Flags = indicateur codé sur 6 bits gauche à droite
   1er = URG        4me = RST
   2me = ACK        5me = SYN
   3me = PSH        6me = FIN
```

Structure du message BLUP

```
<-----------------32bits----------------------->
+-----------------------+-----------------------+
| BLUP ID               | Version BLUP          |
+-----------------------+-----------------------+
```

Structure de datagramme UDP

```
<-----------------32bits----------------------->
+-----------------------+-----------------------+
| Port Source           | Port Destination      |
+-----------------------+-----------------------+
| Longueur UDP          | Somme de ctrl (message)
+-----------------------+-----------------------+
...      Données
+-----------------------------------------------+
```

Quelques services associés aux ports

```
ssh           22/tcp       ssh           22/udp
smtp          25/tcp
domain        53/tcp       domain        53/udp
www           80/tcp       www           80/udp
pop-3        110/tcp       pop-3        110/udp ...
```

DNS

```
< 2o.>< 2o.><2o.>< 2o.><2o.>< 2o.>< Qo.><Ro.>< So.>< Io.>
+-----+-----+----+-----+----+-----+- - -+ - -+- - -+ - - +
|Ident|Flags|NbQu|NbRep|NbSR|NbInf|Quest|Rép.|Serv.|Info.|
+-----+-----+----+-----+----+-----+- - -+ - -+- - -+ - - +

* Ident = Identification d'échange
* Flags = Indicateurs de paramètres DNS. Le bit de poid fort
spécifie si c'est une requete (0) ou une réponse (1).
* NbQu = Nombre de questions
* NbRep = Nombre de champs réponses
* NbSR = Nombre de champs de serveurs DNS de référence
* NbInf = Nombre de champs d'informations additionnelles

Une question:
<----N-octets----><2octets><2octets>
+--- - - - - - ---+--------+--------+
|       Nom       |  Type  | Classe |
+--- - - - - - ---+--------+--------+

Un champ réponse/référence/information:
<Moctets>< 2o. >< 2o. ><4octets>< 2o. ><--D-octets-->
+-- -  --+------+------+--------+------+-- - - - - --+
|  Nom   | Type |Classe| T.T.L. |Taille|  Données    |
+-- -  --+------+------+--------+------+-- - - - - --+

* Nom : chaque nom de label est précédé par un octet indiquant
le nombre de caractères ASCII le composant (si valeur < 63,
sinon 0xC0+N indique un renvoi au Nieme octet par rapport au
début du message DNS de la valeur N de l'octet suivant.
Termine par 0x00.
* Quelques type :                1 = A (adresse IPv4)
  2 = NS (nom de serveur DNS)   5 = CNAME (alias)
  6 = SOA (zone DNS gérée)     15 = MX (serveur de messagerie)
* Classe : 1 = Internet
* T.T.L. : validité en secondes
* Taille : longueur des données en octets
* Données : Nom (pour NS et CNAME)
            Priorité (2 octets) puis Nom (pour MX)
            Adresses (pour A : 4 octets)
```


Ne pas rendre cette feuille

Ne pas rendre cette feuille