1 **Examen Réparti 1 : ARES 2010-2011** 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 *(7 points)*

PlanetLab est une plateforme de recherche permettant de déployer des applications innovantes sur plus de 1000 machines réparties à travers le monde. Afin de fournir le meilleur service aux utilisateurs de la plateforme, il est demandé à l'administrateur de créer une application web permettant de visualiser l'état des machines distantes sur une carte. Cette application web doit également servir à l'administrateur à accéder aux machines à distance pour y exécuter certaines commandes.

1. Afin de vérifier si certains processus sont actifs sur les machines distantes, l'application exécute la commande ps sur ces machines à partir du serveur web.

   (a) Rappelez les différentes caractéristiques des trois protocoles applicatif d'accès à distance les plus connus (nom, protocole transport et port) et justifiez le service de transport utilisé.

   (b) Indiquez les avantages et inconvénients de ces protocoles applicatifs. Précisez celui que l'administrateur devrait utiliser ?

2. Pour gérer les aspects réseau de la plateforme, l'application utilise SNMP entre le serveur web et les machines distantes.

   (a) Quelles commandes du protocole de gestion peuvent être utilisées pour récupérer ou modifier l'état des machines distantes et permettre à ces machines d'envoyer des alertes (trafic dépassant certaines limites, interfaces déconnectées...).

   (b) Préciser pourquoi le protocole de transport UDP est utilisé et quel problème principal cela introduit en terme de service à l'application. Comment celui-ci est-il résolu ?

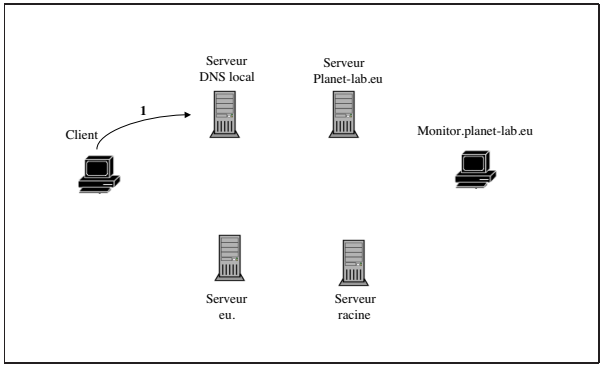
3. Lorsqu'une alerte est interceptée sur le serveur web, l'application doit envoyer un e-mail aux administrateurs des machines distantes concernées.

   (a) Pouvez vous rappeler le protocole applicatif utilisé pour l'envoi d'e-mail et indiquer ses limitations.

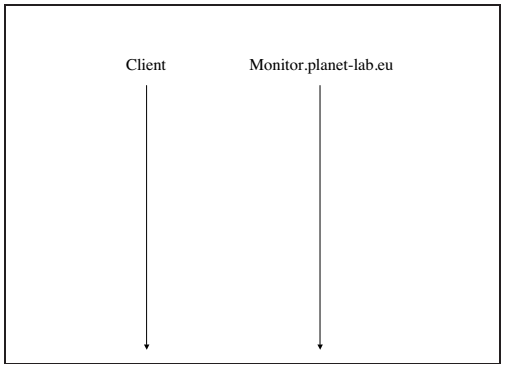
   (b) Quels sont les protocoles utilisés pour récupérer ces e-mails et indiquez leurs principales différences. Le serveur de l'application a peu de ressources de stockage, indiquez lequel des protocoles précédent est le plus adapté (justifiez).

4. Le site web de l'application permet d'avoir accès à une carte donnant différentes valeurs sur les machines distantes.

   (a) Sachant que le cache du serveur DNS local est vide et que la requête DNS est itérative, indiquez sur le schéma ci-contre les échanges DNS effectuées pour obtenir l'adresse associée au nom `monitor.planet-lab.eu`.



   (b) La page d'accueil étant composée d'un fichier HTML et de 2 images (carte.png, logo.gif). Tracez le chronogramme des connexions utilisées pour récupérer la page web du serveur `monitor.planet-lab.eu`, sachant que le serveur web utilise le protocole HTTP 1.1 en mode persistant sans pipeline.



2

Examen Réparti 1 : ARES 2010-2011

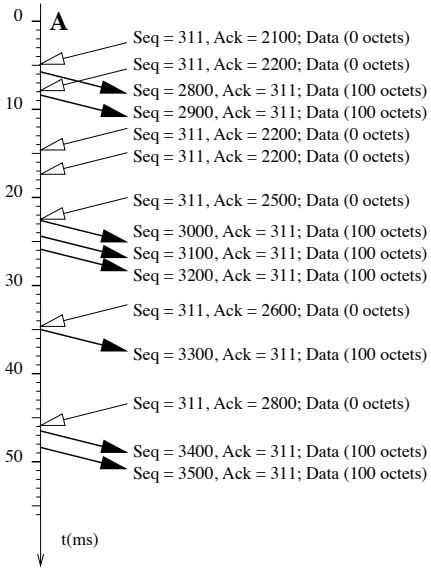
Durée totale: *2h00*
Autorisé: *Une feuille A4 manuscrite*
Non autorisés: *Autres documents, calculatrices, téléphones portables, PDA, etc.*

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 TCP *(7 points)*

Scénario 1 :
Le chronogramme ci-dessous représente les messages échangés pendant un intervalle de temps inclus dans la durée totale d'une connexion TCP entre les machines A et B. Les échanges sont observés au niveau de l'interface réseau de **A** (les flèches blanches indiquent les segments reçus et les noires ceux émis).

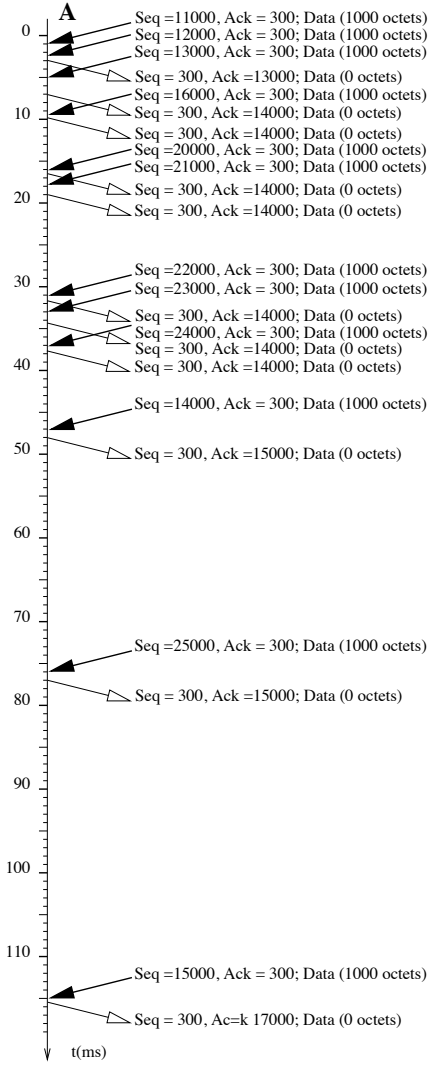


Hypothèses :

- l'échelle de temps du chronogramme a pour origine le début de la capture ;
- les numéros de séquences sont directement ceux observés dans les segments ;
- le flag ACK est toujours positionné, le flag PSH lorqu'il y a des données de taille non nulle dans le segment.

1. Dans quel état se trouve la connexion TCP dans l'intervalle de temps étudié ? Justifiez votre réponse.
2. Quelles données TCP sont émises (et par quelle machine) lors de l'échange représenté ici ? Justifiez votre réponse.
3. De quelles données TCP a-t-on la confirmation de leur réception ? Justifiez votre réponse.
4. Quelle événement antérieur déclenche l'émission de 3 segments vers t=22ms ? Justifiez votre réponse.
5. Quelle événement antérieur déclenche l'émission de 2 segments vers t=46ms ? Justifiez votre réponse.
6. Quelles hypothèses peut-on faire sur la taille de la fenêtre d'émission ? Justifiez votre réponse.

Scénario 2 :
Le chronogramme ci-dessous présente également une partie des échanges d'une connexion TCP entre A et B. L'observation est toujours effectuée au niveau de **A** (attention, pour ce scénario, les flèches noires indiquent les réceptions alors que les blanches les émissions).



Les hypothèses sont similaires à celles du scénario précédent.

1. Quelles sont les données reçut par **A** lors de l'intervalle de temps représenté ? A quelles données émises par **B** correspondent-elles ?
2. Quelles hypothèses fait **B** en recevant l'acquittement émis à t=10ms ? Ces situations sont-elles envisageables par **A** ?
3. Quelles hypothèses fait **B** en recevant l'acquittement émis à t=16ms ? Ces situations sont-elles envisageables par **A** ?
4. Justifiez la réception du segment à t=47ms en précisant l'évenement déclencheur.
5. Estimez le RTT *(Round Trip Time)* entre **A** et **B**. Justifiez en précisant l'échange choisi prouvant cette valeur.
6. Justifiez la réception du segment à t=76ms en précisant l'évenement déclencheur.
7. Pouvez-vous estimer la taille de la fenêtre d'émission de **B** ? Si oui, indiquez-là et justifiez sa valeur.
8. Justifiez la réception par du segment à t=115ms en précisant l'évenement déclencheur.

3

Examen Réparti 1 : ARES 2010-2011

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 des différents niveaux protocolaires d'une trame *(7 points)*

1. Voici la trace d'une 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 15 17 78 8a 4a 00 15  17 50 b4 bf 08 00 45 00   ...x.J.. .P....E.
0010  00 f8 c8 08 00 00 40 11  9a df 0a 06 02 01 0a 06   ......@. ........
0020  01 01 00 35 a9 31 00 e4  73 8b 72 1e 81 80 00 01   ...5.1.. s.r.....
0030  00 02 00 03 00 05 07 6c  65 6d 6f 6e 64 65 02 66   .......l emonde.f
0040  72 00 00 0f 00 01 c0 0c  00 0f 00 01 00 00 70 80   r....... ......p.
0050  00 0a 00 05 05 73 6d 74  70 30 c0 0c c0 0c 00 0f   .....smt p0......
0060  00 01 00 00 70 80 00 0a  00 0a 05 73 6d 74 70 31   ....p... ...smtp1
0070  c0 0c c0 0c 00 02 00 01  00 00 18 7a 00 14 03 6e   ........ ...z...n
0080  73 62 0a 62 6f 6f 6b 6d  79 6e 61 6d 65 03 63 6f   sb.bookm yname.co
0090  6d 00 c0 0c 00 02 00 01  00 00 18 7a 00 06 03 6e   m....... ...z...n
00a0  73 61 c0 58 c0 0c 00 02  00 01 00 00 18 7a 00 06   sa.X.... .....z..
00b0  03 6e 73 63 c0 58 c0 2a  00 01 00 01 00 00 02 58   .nsc.X.* .......X
00c0  00 04 c2 03 51 05 c0 40  00 01 00 01 00 00 02 58   ....Q..@ .......X
00d0  00 04 c2 03 51 06 c0 74  00 01 00 01 00 00 56 36   ....Q..t ......V6
00e0  00 04 58 bf f9 87 c0 54  00 01 00 01 00 00 56 36   ..X....T ......V6
00f0  00 04 d9 18 52 22 c0 86  00 01 00 01 00 00 56 36   ....R".. ......V6
0100  00 04 c3 9a e4 e5                                 ......
```


2. Y-a-t-il des options IP et des options TCP ? Quelles sont-elles ?

3. Quel est le numéro de version utilisée du protocole BLUP ?

4. Quelles sont les adresses IP du poste client et du serveur ?

5. Vérifiez que la trace présente l'intégralité des octets de la trame émise sur le réseau. Justifiez votre réponse

6. Pour quelle(s) raison(s) peut-on être sûr d'être en présence d'un message de réponse DNS ?

7. Quelle application a pus déclencher l'échange DNS ?

8. A quoi sert le champ d'identification (`Ident`) du message applicatif ?

9. Que vous apprend le message DNS (réponses/références/informations) ?

Nom	Type	Données

10. Quel est le serveur de noms de référence *(authoritative server)* primaire pour l'institution ciblée ?

11. Le serveur Web de l'institution ciblée est-il hébergé sur la même machine que son serveur de messagerie ?

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                 8 = EGP
        2 = IGMP                11 = BLUP
        4 = IP (encapsulation)  17 = UDP
```

Structure du message BLUP

```
<-----------------32bits----------------------->
+-----------------------+-----------------------+
| Port Source           | Port Destination      |
+-----------------------+-----------------------+
| Longueur BLUP         | Version BLUP          |
+-----------------------+-----------------------+
...      Données
+---------------------------------------------+
```

Structure de datagramme UDP

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

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
+-----------------------------------------------+
```

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 = Identificateur 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