

ARES/NetArch — 2012-2013

Examen réparti 1 : Sujet version A en Français

App

Durée totale : 2h00

Autorisé : Une feuille A4 manuscrite

Non autorisés : Autres documents, calculatrices, téléphones portables, 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 ne devez pas écrire votre nom sur les feuilles rendues).

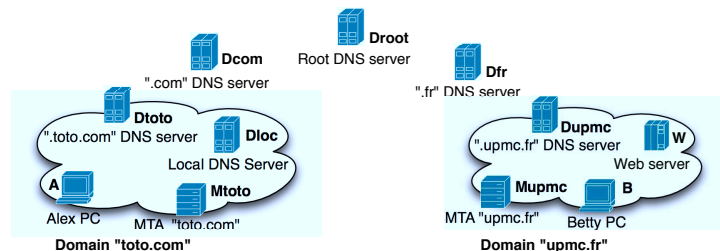
Vous devez noter vos réponses directement sur ce sujet dans les cadres correspondants.

App

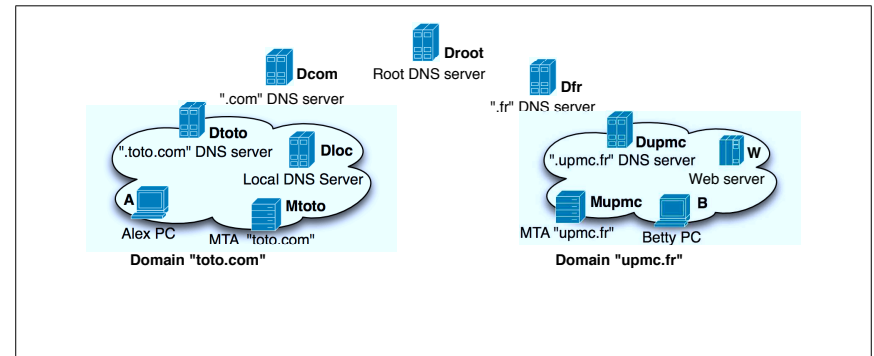
1 Applications (7 points)

Les questions suivantes sont relatives aux échanges applicatifs et seulement eux. Chaque question présente une figure qui indique les hôtes impliqués (pour les référencer, utilisez le nom abrégé de ces hôtes imprimé en **gras**). Pour répondre aux questions, il est nécessaire de compléter ces figures en identifiant clairement les messages échangés (par exemple en les numérotant). **Puis vous devez justifier votre réponse dans le reste du cadre.**

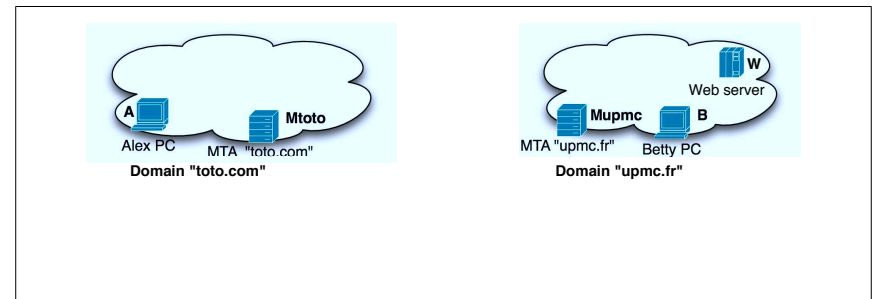
1. Alex veut envoyer un e-mail à Betty (betty@upmc.fr). Alex et Betty gèrent leurs e-mail à partir de leurs PC avec des clients de messagerie classiques (MTA). Les PC des utilisateurs ne mémorisent pas les correspondances nom/adresse et le serveur DNS local (**Dloc**) ne connaît que les adresses des hôtes de son domaine. Indiquez **seulement les messages DNS** qu'impliquerait l'envoi de l'e-mail. Expliquez pourquoi ces messages sont envoyés.



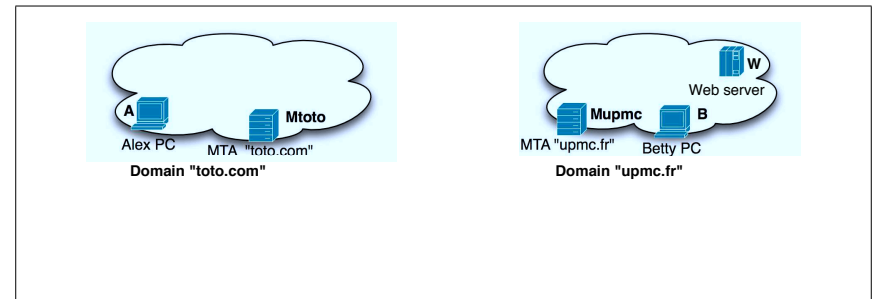
2. Avec les mêmes hypothèses qu'à la question précédente, sauf pour le serveur DNS local (**Dloc**) qui connaît cette fois, en plus des adresses IP des hôtes de son domaine, l'adresse du serveur de nom de référence de la zone "upmc.fr" (**Dupmc**). Indiquez **seulement les messages DNS** qu'impliquerait l'envoi de l'e-mail dans ces conditions. Expliquez les changements.



3. En supposant que tous les échanges DNS réussissent, indiquez maintenant **seulement les messages SMTP** qu'impliquerait l'envoi de l'e-mail de Alex vers Betty **si une erreur** dans le nom de la boîte aux lettres du destinataire provoque un échec (par exemple bety@upmc.fr). Justifiez les messages proposés.



4. En supposant toujours que tous les échanges DNS réussissent, indiquez maintenant **seulement les messages SMTP et POP** qu'impliquerait l'envoi de l'e-mail de Alex vers Betty **sans erreur** et si le récepteur utilise POP pour la remise finale. Justifiez les messages proposés.



Trp

ARES/NetArch — 2012-2013

Examen réparti 1 : Sujet version A en Français

Durée totale : 2h00

Autorisé : Une feuille A4 manuscrite

Non autorisés : Autres documents, calculatrices, téléphones portables, etc.

Trp

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 ne devez pas écrire votre nom sur les feuilles rendues).

Vous devez noter vos réponses directement sur ce sujet dans les cadres correspondants.

2 Couche transport (6 points)

1. Quel est le rôle des protocoles de la couche transport ?

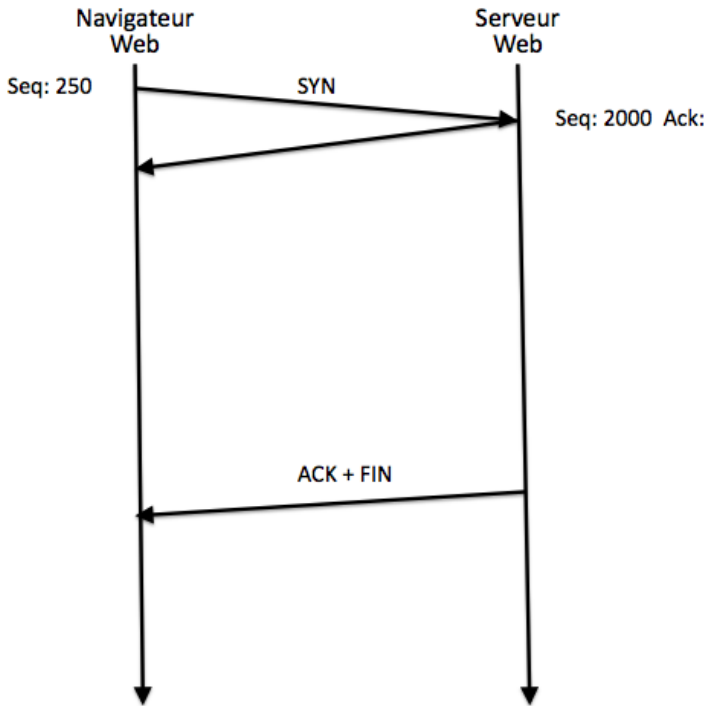
2. Est-ce que les routeurs du réseau Internet peuvent émettre des messages TCP ou UDP ? Justifiez votre réponse.

3. Dans TCP, quel est le rôle du RTO et comment est-il calculé ? Quel est l'impact sur TCP d' une sous-évaluation ou d'une sur-évaluation du RTO ?

4. Comparez dans le tableau suivant les fonctionnalités, complexités, performances et le coût réseau de TCP et UDP

	TCP	UDP
Fonctionnalités		
Complexités		
Performances		
Coûts		

5. Un navigateur web se connecte sur un serveur web pour récupérer une page HTML de 1050 octets. La commande envoyée est un "GET" faisant 100 octets. Sachant que la fenêtre de réception est de 1500 octets et qu'un MSS est de 500 octets, indiquez sur le chronogramme suivant les différentes connexions, leur type, le nombre d'octets envoyé ainsi que leur numéro de séquence et d'acquittement



ARES/NetArch — 2012-2013

Examen réparti 1 : Sujet version A en Français

Frm

Durée totale : 2h00

Autorisé : Une feuille A4 manuscrite

Non autorisés : Autres documents, calculatrices, téléphones portables, 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 ne devez pas écrire votre nom sur les feuilles rendues).

Vous devez noter vos réponses directement sur ce sujet dans les cadres correspondants.

3 Analyse protocolaire (7 points)

Dans cette partie, la trace de deux trames Ethernet est présentée en trois colonnes de manière identique à celles étudiées dans les labs.

1. Délimitez et identifiez soigneusement les champs de tous les niveaux protocolaires (utilisez si possible une couleur par protocole) afin de répondre aux questions suivantes. Vous disposez pour cela de l'**Annexe** page 7. Si la valeur d'un champ est importante pour la compréhension de l'échange ou pour la vérification du décodage, indiquez-la dans sa représentation standard.

```
0000 00 24 d4 b4 09 a6 54 42 49 88 fd cd 08 00 45 00 .$. . . . TB I . . . . E.
0010 00 3e 69 e5 00 00 40 11 53 0b c0 a8 00 0a d4 1b .>i . . . @. S . . . . .
0020 28 f1 d6 39 00 35 00 2a bc 9a b8 d1 01 00 00 01 (.9.5.* . . . . .
0030 00 00 00 00 00 00 03 77 77 77 08 66 61 63 65 62 . . . . . w ww.faceb
0040 6f 6f 6b 03 63 6f 6d 00 00 01 00 01 . . . . . ook.com. . . .
```

```
0000 54 42 49 88 fd cd 00 24 d4 b4 09 a6 08 00 45 00 TBI . . . $ . . . . . E.
0010 00 a8 01 e7 00 00 39 11 c1 9f d4 1b 28 f1 c0 a8 . . . . . 9. . . . ( . .
0020 00 0a 00 35 d6 39 00 94 93 79 b8 d1 81 80 00 01 . . 5.9 . . y . . . .
0030 00 02 00 02 00 02 03 77 77 77 08 66 61 63 65 62 . . . . . w ww.faceb
0040 6f 6f 6b 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 ook.com. . . . .
0050 00 01 00 00 06 24 00 0b 03 77 77 77 04 63 31 30 . . . . . $. . . www.c10
0060 72 c0 10 c0 2e 00 01 00 01 00 00 06 25 00 04 1f r . . . . . % . . .
0070 0d 51 04 c0 32 00 02 00 01 00 02 4c 0a 00 07 01 .Q . 2 . . . . L . . .
0080 61 02 6e 73 c0 32 c0 32 00 02 00 01 00 02 4c 0a a.ns.2.2 . . . . . L.
0090 00 04 01 62 c0 57 c0 55 00 01 00 01 00 02 53 cb . . . b.W.U . . . . . S.
00a0 00 04 45 ab ef 0b . . E . . .
```

2. Vérifiez si les traces présentent l'intégralité des octets des trames émises sur le réseau. Justifiez votre réponse.

3. Combien d'adresses IP sont apparues dans l'échange des deux trames précédentes ? A quoi chaque adresse correspond-elle ?

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

5. Quelle action de la couche application a pu déclencher cet échange ?

6. Est-ce que le RTT pourrait être calculé à partir des deux traces ? Justifiez votre réponse.

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 | FI | 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)
FI (3 premiers bits) = indicateurs pour la fragmentation
(Réservé|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 = NVP-II
2 = IGMP 17 = UDP
6 = TCP 41 = IPv6

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

Options = suites d'option codées sur
* 1 octet à 00 = Fin des options
* 1 octet à 01 = NOP (pas d'opération)
* plusieurs octets de type TLV
T = un octet de type:
2 Négociation de la taille max. du segment
3 Adaptation de la taille de la fenêtre
8 Estampilles temporelles
L = un octet pour la taille totale de l'option
V = valeur de l'option (sur L-2 octets)

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

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 poids fort spécifie si c'est une requête (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.
Terminer 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
