ARES/NetArch — 2013-2014

App

Examen réparti 1 : Sujet version A en Français

App

Durée totale : *2h00*
Autorisé : *Une feuille A4 manuscrite (recto/verso)*
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.

1 Applications (6 points)

Les questions de cette section sont relatives aux échanges applicatifs et seulement eux. Voici dans la suite une série de messages qui ont été interceptés dans un réseau (chaque ligne correspond à un message) :

```
220 Welcome to file.srv.net.
USER anonymous
331 Please specify the password.
PASS alice@wonderland.org
230 Login successful.
SYST
215 UNIX Type: L8
CWD pub
250 Directory successfully changed.
PASV
227 Entering Passive Mode (156,42,2,1,10,28).
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (156,42,2,1,10,29).
RETR rabbit.txt
150 Opening BINARY mode data connection for rabbit.txt (28520 bytes).
226 File send OK.
QUIT
221 Goodbye.
```

1. A quel type d'application et à quel protocole applicatif correspond cet échange de messages ?

2. Quelle est l'identité de l'utilisateur de ce service ? Précisez s'il s'est authentifié ?

3. Quel est l'intérêt d'accéder à ce service avec cette identité ?

4. Quelles actions a réalisé l'utilisateur durant cet échange ?

5. Deux commandes PASV apparaissent dans l'exemple présenté ci-dessus. Pouvez-vous préciser leur intérêt puis expliciter les valeurs et usages des paramètres utilisée dans le cadre de cet exemple ?

6. Dans quelle situation ces commandes sont généralement utilisées à la place de commandes PORT ? Justifiez.

7. Pourquoi les 2 commandes qui suivent les commandes PASV sont chacune suivies de 2 messages ? Justifiez dans le cas de notre exemple.

8. Pour pouvoir réaliser l'échange applicatif précédent, d'autres protocoles peuvent être utilisés simultanément pour le bon déroulement de celui-ci. En supposant que les machines client (`PC24.upmc.fr`) et serveur (`file.srv.net`) de l'échange ci-dessus sont connues de l'utilisateur uniquement par leurs noms littéraux, faites un schéma en indiquant toutes les machines impliquées et tous les messages applicatifs échangés (à l'aide de flèches) lors de la réalisation de l'échange[1].

[1] Les noms des machines potentiellement impliquées sont : $PC24$ (le client `PC24.upmc.fr` de l'échange précédent) ; DNS_{PC24} (le serveur DNS local de $PC24$) ; DNS_{upmc} (le serveur DNS de référence de `.upmc.fr`) ; DNS_{fr} (le serveur DNS de référence de `.fr`) ; DNS_{root} (le serveur DNS de référence racine) ; DNS_{net} (le serveur DNS de référence de `.net`) ; DNS_{srv} (le serveur DNS de référence de `.srv.net`) ; DNS_{file} (le serveur DNS local des machines de `.srv.net`) ; $FILE$ (le serveur `file.srv.net` de l'échange précédent) ; et WWW (le serveur web `www.server.net` associé à `.srv.net`).

ARES/NetArch — 2013-2014

Trp

Examen réparti 1 : Sujet version A en Français

Trp

Durée totale : *2h00*
Autorisé : *Une feuille A4 manuscrite (recto/verso)*
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.

2 Couche transport (7 points)

1. **UDP** : Quels services propose UDP à la couche application par rapport à IP ? Précisez leur intérêt.

2. **Fiabilité :**
   (a) Quels mécanismes sont utilisés au niveau de la couche transport afin de détecter et récupérer des paquets corrompus (les paquets qui ont des erreurs de bits) ?
   (b) Quel mécanisme est utilisé au niveau de la couche transport afin de détecter les paquets dupliqués ?
   (c) Quels mécanismes sont utilisés au niveau de la couche transport afin de faire face à des pertes de paquets ?
   (d) Quels mécanismes sont utilisés au niveau de la couche transport afin de permettre la transmission fiable d'un grands nombres de paquets non acquittés (qui sont «en vol», *"in-flight"* en anglais) ?

3. **Connexions :**
   (a) Avec la pile TCP/IP classique, quel est le rôle des routeurs pour maintenir une connexion de bout en bout ?
   (b) Comment une application qui fonctionne sur UDP peut maintenir une connexion ?
   (c) Décrivez brièvement comment une connexion est ouverte par TCP
   (d) Décrivez brièvement deux façons dont une connexion est fermée par TCP
   (e) Un navigateur web se connecte sur un serveur web pour récupérer une page HTML de 900 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, dessinez un chronogramme indiquant tous les différents messages TCP échangés (avec leur type, le nombre d'octets envoyés ainsi que leur numéro de séquence et d'acquittement).

ARES/NetArch — 2013-2014

Frm

Examen réparti 1 : Sujet version A en Français

Frm

Durée totale : *2h00*
Autorisé : *Une feuille A4 manuscrite (recto/verso)*
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)

Etudiez la trame qui est donnée dans l'**Annexe 1** (page 7) et répondez aux questions suivantes en **justifiant soigneusement** vos réponses. Vous disposez également de l'**Annexe 2** (page 9) pour vous aider dans l'analyse.

1. Faites un schéma sur lequel figurent les différents équipements impliqués dans l'envoi de cette trame, ainsi que toutes les adresses et les numéros de port apparaissant dans cette trame.

2. Quelles sont les commandes applicatives qui ont été nécessairement émises préalablement à l'envoi de cette trame ?

3. Pouvez-vous lister de façon exhaustive ce que contient le message applicatif ?

4. Le message applicatif a-t-il été envoyé au moyen de cette seule trame ou de plusieurs trames ?

5. Que doit faire le destinataire du message applicatif pour pouvoir en prendre connaissance ? Listez toutes les possibilités et pour l'une d'entre elles (que vous choisirez), donnez toutes les commandes applicatives qui devront nécessairement être utilisées.

6. Donnez le codage en hexadécimal (dump) de la prochaine trame que va recevoir l'émetteur de cette trame (vous mettrez "XX" pour les octets dont vous ne pouvez pas calculer la valeur).

Annexe 1

Dans cette partie, la trace d'une trame Ethernet est présentée en trois colonnes de manière identique à celle étudiée dans les labs. Pour l'analyser, vous disposez de l'**Annexe 2** (page 9).

```
0000   00 50 7f 05 7d 40 08 00 46 b1 49 5e 08 00 45 00  .P..}@..F.I^..E.
0010   05 a2 98 a8 40 00 80 06 76 48 0a 21 02 01 3e 3e  ....@...vH.!..>>
0020   9c 05 04 57 00 19 ab a9 13 5b 37 ad eb ec 50 10  ...W.....[7...P.
0030   fb 25 4f 23 00 00 4d 65 73 73 61 67 65 2d 49 44  .%O#..Message-ID
0040   3a 20 3c 34 31 37 32 42 39 31 33 2e 36 30 30 30  : <4172B913.6000
0050   37 30 32 40 66 72 65 65 2e 66 72 3e 0d 0a 44 61  702@free.fr>..Da
0060   74 65 3a 20 53 75 6e 2c 20 31 37 20 4f 63 74 20  te: Sun, 17 Oct
0070   32 30 30 34 20 32 30 3a 32 35 3a 32 33 20 2b 30  2004 20:25:23 +0
0080   32 30 30 0d 0a 46 72 6f 6d 3a 20 45 6e 73 65 69  200..From: Ensei
0090   67 6e 61 6e 74 20 52 45 53 20 3c 62 6f 69 74 65  gnant RES <boite
00a0   72 65 73 32 30 30 34 40 66 72 65 65 2e 66 72 3e  res2004@free.fr>
00b0   0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f  ..User-Agent: Mo
00c0   7a 69 6c 6c 61 20 54 68 75 6e 64 65 72 62 69 72  zilla Thunderbir
00d0   64 20 30 2e 38 20 28 57 69 6e 64 6f 77 73 2f 32  d 0.8 (Windows/2
00e0   30 30 34 30 39 31 33 29 0d 0a 58 2d 41 63 63 65  0040913)..X-Acce
00f0   70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d  pt-Language: en-
0100   75 73 2c 20 65 6e 0d 0a 4d 49 4d 45 2d 56 65 72  us, en..MIME-Ver
0110   73 69 6f 6e 3a 20 31 2e 30 0d 0a 54 6f 3a 20 20  sion: 1.0..To:
0120   6f 6c 69 76 69 65 72 2e 66 6f 75 72 6d 61 75 78  olivier.fourmaux
0130   40 6c 69 70 36 2e 66 72 0d 0a 53 75 62 6a 65 63  @lip6.fr..Subjec
0140   74 3a 20 54 65 73 74 0d 0a 43 6f 6e 74 65 6e 74  t: Test..Content
0150   2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74  -Type: multipart
0160   2f 6d 69 78 65 64 3b 0d 0a 20 62 6f 75 6e 64 61  /mixed;.. bounda
0170   72 79 3d 22 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d  ry="------------
0180   30 39 30 32 30 33 30 39 30 31 30 36 30 33 30 30  0902030901060300
0190   30 33 30 30 30 30 30 32 22 0d 0a 0d 0a 54 68 69  03000002"....Thi
01a0   73 20 69 73 20 61 20 6d 75 6c 74 69 2d 70 61 72  s is a multi-par
01b0   74 20 6d 65 73 73 61 67 65 20 69 6e 20 4d 49 4d  t message in MIM
01c0   45 20 66 6f 72 6d 61 74 2e 0d 0a 2d 2d 2d 2d 2d  E format...-----
01d0   2d 2d 2d 2d 2d 2d 2d 2d 2d 30 39 30 32 30 33 30  ---------0902030
01e0   39 30 31 30 36 30 33 30 30 30 33 30 30 30 30 30  9010603000300000
01f0   32 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a  2..Content-Type:
0200   20 74 65 78 74 2f 70 6c 61 69 6e 3b 20 63 68 61   text/plain; cha
0210   72 73 65 74 3d 49 53 4f 2d 38 38 35 39 2d 31 3b  rset=ISO-8859-1;
0220   20 66 6f 72 6d 61 74 3d 66 6c 6f 77 65 64 0d 0a   format=flowed..
0230   43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 65 72  Content-Transfer
0240   2d 45 6e 63 6f 64 69 6e 67 3a 20 37 62 69 74 0d  -Encoding: 7bit.
0250   0a 0d 0a 56 6f 69 63 69 20 75 6e 20 65 78 65 6d  ...Voici un exem
0260   70 6c 65 20 64 65 20 6d 65 73 73 61 67 65 20 4d  ple de message M
0270   49 4d 45 20 61 76 65 63 20 69 6d 61 67 65 20 6a  IME avec image j
0280   6f 69 6e 74 65 2e 0d 0a 0d 0a 2d 2d 2d 2d 2d 2d  ointe.....------
0290   2d 2d 2d 2d 2d 2d 2d 2d 30 39 30 32 30 33 30 39  --------09020309
02a0   30 31 30 36 30 33 30 30 30 33 30 30 30 30 30 32  0106030003000002
02b0   0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20  ..Content-Type:
02c0   69 6d 61 67 65 2f 70 6e 67 3b 0d 0a 20 6e 61 6d  image/png;.. nam
02d0   65 3d 22 6f 70 65 6e 6c 6f 67 6f 2d 6e 64 2d 35  e="openlogo-nd-5
```

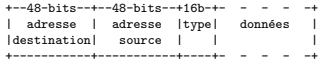


```
02e0   30 2e 70 6e 67 22 0d 0a 43 6f 6e 74 65 6e 74 2d  0.png"..Content-
02f0   54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e  Transfer-Encodin
0300   67 3a 20 62 61 73 65 36 34 0d 0a 43 6f 6e 74 65  g: base64..Conte
0310   6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20  nt-Disposition:
0320   69 6e 6c 69 6e 65 3b 0d 0a 20 66 69 6c 65 6e 61  inline;.. filena
0330   6d 65 3d 22 6f 70 65 6e 6c 6f 67 6f 2d 6e 64 2d  me="openlogo-nd-
0340   35 30 2e 70 6e 67 22 0d 0a 0d 0a 69 56 42 4f 52  50.png"....iVBOR
0350   77 30 4b 47 67 6f 41 41 41 41 4e 53 55 68 45 55  w0KGgoAAAANSUhEU
0360   67 41 41 41 44 49 41 41 41 41 39 43 41 4d 41 41  gAAADIAAAA9CAMAA
0370   41 44 59 74 38 70 57 41 41 41 41 4d 31 42 4d 56  ADYt8pWAAAAM1BMV
0380   45 58 2f 2f 2f 2f 48 41 44 62 4c 45 45 50 6a 66  EX////HADbLEEPjf
0390   35 72 37 0d 0a 37 2f 4c 71 6e 37 50 78 76 38 33  5r7..7/Lqn7Pxv83
03a0   56 51 47 6a 34 33 2b 62 63 59 49 4c 30 7a 39 6e  VQGj43+bcYILOz9n
03b0   74 72 38 44 4f 49 45 2f 53 4d 46 7a 67 63 49 37  tr8DOIE/SMFzgcI7
03c0   6d 6a 36 66 5a 55 48 58 41 2b 4b 79 58 41 41 41  mj6fZUHXA+KyXAAA
03d0   41 41 57 4a 4c 52 30 51 41 69 41 55 64 0d 0a 53  AAWJLR0QAiAUd..S
03e0   41 41 41 41 41 6c 77 53 46 6c 7a 41 41 41 4c 45  AAAAAlwSFlzAAALE
03f0   67 41 41 43 78 49 42 30 74 31 2b 2f 41 41 41 41  gAACxIB0t1+/AAAA
0400   41 64 30 53 55 31 46 42 39 49 42 41 68 59 48 48  Ad0SU1FB9IBAhYHH
0410   45 65 67 34 2f 55 41 41 41 4a 4b 53 55 52 42 56  Eeg4/UAAAJKSURBV
0420   48 69 63 6c 56 5a 4a 0d 0a 67 6f 51 67 44 45 54  HiclVZJ..goQgDET
0430   43 6a 69 44 2f 66 2b 30 6b 67 44 61 62 4f 74 61  CjiD/f+0kgDabOta
0440   70 47 79 6d 53 79 67 61 4d 7a 52 44 53 51 32 51  pGymSygaMzRDSQ2Q
0450   57 6c 46 68 38 58 4d 46 45 76 68 46 34 30 4a 70  WlFh8XMFEvhF40Jp
0460   62 2f 30 35 54 61 52 74 67 7a 62 4f 46 69 55 44  b/05TaRtgzbOFiUD
0470   51 0d 0a 6e 4b 73 37 78 73 46 58 6a 49 79 77 4a  Q..nKs7xsFXjIywJ
0480   4c 6e 39 6c 6b 43 41 6d 53 47 62 7a 30 6c 48 72  Ln9lkCAmSGbz0lHr
0490   78 41 65 64 43 4e 71 6a 45 54 44 30 4b 35 5a 46  xAedCNqjETD0K5ZF
04a0   2f 49 79 48 73 51 64 77 34 37 32 59 66 6e 46 58  /IyHsQdw472YfnFX
04b0   78 36 76 38 75 44 4f 73 4c 52 36 0d 0a 7a 72 56  x6v8uDOsLR6..zrV
04c0   6a 46 5a 65 47 38 34 75 62 72 53 4c 6b 58 61 35  jFZeG84ubrSLkXa5
04d0   50 7a 6e 34 75 6d 45 63 54 6e 65 63 79 69 31 4e  Pzn4umEcTnecyi1N
04e0   46 48 33 63 50 44 4d 5a 69 59 30 59 79 78 64 38  FH3cPDMZiY0Yyxd8
04f0   5a 54 47 54 58 65 4e 6c 6d 2f 6d 47 44 6c 56 42  ZTGTXeNlm/mGDlVB
0500   62 77 58 4f 52 0d 0a 32 6a 34 55 46 78 79 6d 66  bwXOR..2j4UFxymf
0510   7a 44 44 67 5a 4b 67 73 73 56 4a 75 59 41 53 6f  zDDgZKgssVJuYASo
0520   36 62 30 36 65 68 67 55 44 2f 49 6c 52 45 4d 4b  6b06ehgUD/IlREMK
0530   72 61 58 63 67 70 32 65 61 37 6c 6a 51 4b 7a 36  raXcgp2ea7ljQKz6
0540   51 4d 70 45 52 50 6a 4b 67 50 70 36 77 39 46 0d  QMpERPjKgPp6w9F.
0550   0a 47 35 57 73 34 6f 66 43 46 6e 76 62 55 35 64  .G5Ws4ofCFnvbU5d
0560   72 2b 57 78 58 7a 4f 30 39 67 2b 6e 4e 73 77 58  r+WxXzO09g+nNswX
0570   6f 63 4f 4b 6e 57 62 79 66 69 7a 6b 6a 56 49 71  ocOKnWbyfizkjVIq
0580   64 78 64 74 74 50 53 47 6f 33 54 51 72 47 65 72  dxdttPSGo3TQrGer
0590   46 69 79 30 4e 65 34 38 66 0d 0a 35 61 69 55 66  Fiy0Ne48f..5aiUf
05a0   67 4e 4d 62 52 35 37 4c 54 43 70 68 37 56 34 74  gNMbR57LTCph7V4t
```

Annexe 2

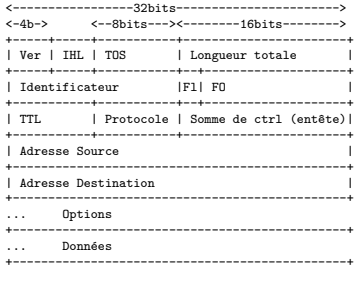
Structure de la trame Ethernet

Trame présentée sans préambule ni CRC :



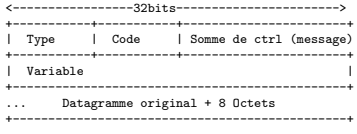

```
Quelques types : 0x0800 = DoD Internet (IPv4)
                 0x0806 = ARP
```

Structure du paquet IPv4



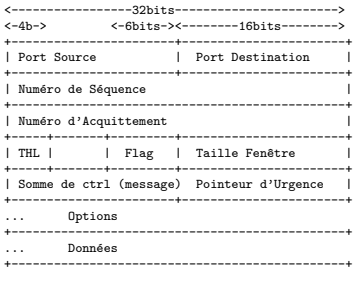

```
Ver = Version d'IP
IHL = Longueur de l'en-tête IP (en mots de 32 bits)
TOS = Type de service
Longueur totale du paquet IP (en octets)
Fl (3 premiers bits) = indicateurs pour la fragmentation
   (Reservé|Ne pas fragmenter|Fragment suivant existe)
FO (13 bits suivants) = Décalage du fragment
 * valeur a multiplier par 8 octets
TTL = Durée de vie restante
Quelques protocoles transportés :
        1 = ICMP           11 = NVP-II
        2 = IGMP           17 = UDP
        6 = TCP            41 = IPv6
```

Structure du datagramme ICMP




```
Quelques types ICMP:  0 = Echo request
                      8 = Echo response
                     11 = Time exceed
```

Structure de segment TCP




```
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

Quelques services associés aux ports

```
ftp-data      20/tcp
ftp           21/tcp
ssh           22/tcp
telnet        23/tcp
smtp          25/tcp
                              domain        53/udp
                              tftp          69/udp
www           80/tcp
                              snmp         161/udp
                              snmp-trap    162/udp
```


Ne pas rendre cette feuille

Ne pas rendre cette feuille