

Examen LI338 « Introduction aux réseaux »
Lundi 15 décembre 2008 – Durée : 2 heures
Autorisés : 1 feuille au format A4 manuscrite + Calculatrice

Voici 6 feuilles (dont une page d'annexe) contenant les énoncés et les zones de réponse à compléter (sans déborder). A la fin de l'épreuve, vous devez nous rendre le tout dans une copie double d'examen vierge.
Afin de garantir l'anonymat, **vous ne devez écrire vos nom, prénom, N° de carte d'étudiant que sur la copie double** et dans le cadre réservé à cet usage.
Des autocollants avec un même numéro aléatoire vous seront distribués pendant l'épreuve : vous en collerez **un sur la copie double** et **un sur chaque feuille du sujet**.

Exercice 1 : Techniques de transmission (4 points)

Un signal porteur d'information de fréquences strictement inférieures à 15 kHz est numérisé. Chaque échantillon produit est ensuite codé sur 16 bits. Le message numérique ainsi produit est ensuite transmis en bande de base.

1. Quelle fréquence d'échantillonnage f_e faut-il utiliser si l'on veut minimiser le débit binaire du message numérique produit à l'issue de l'opération de numérisation ? Justifiez.

2. Quelle capacité C le canal de transmission devra-t-il posséder au minimum pour permettre la transmission de ce message numérique ?

3. On utilise pour la transmission un câble de bande passante $[0, 200 \text{ kHz}]$. Le rapport signal-à-bruit S/N mesuré à la réception est de 18 dB. La transmission est-elle théoriquement possible ? Justifiez.

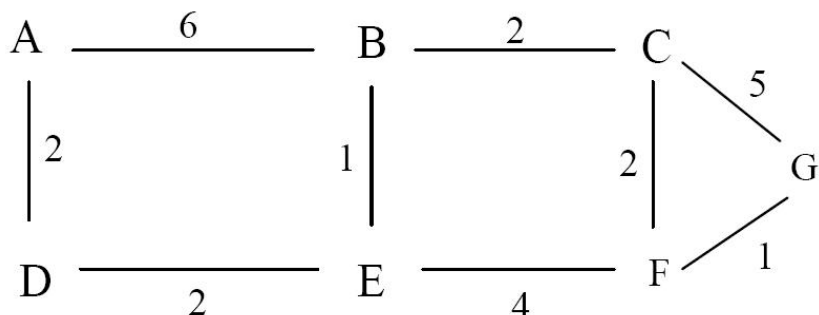
4. Peut-on utiliser un code NRZ binaire pour réaliser la transmission ? Pourquoi ?

5. Peut-on utiliser un code NRZ-8 pour réaliser la transmission ? Pourquoi ?

6. La transmission à l'aide d'un signal NRZ-8 est-elle optimale ? Pourquoi ? Si ce n'est pas le cas, proposer la modulation NRZ M -aire la plus adéquate. A quel débit binaire la liaison va-t-elle fonctionner ?

Exercice 2 : Routage (4 points)

On considère le réseau suivant :



1. Appliquez l'algorithme de Dijkstra pour le nœud A sur le réseau ci-dessus. Indiquez dans quel ordre les sommets ont été traités par l'algorithme (sans donner plus de détails) et dessinez l'arbre couvrant obtenu pour le nœud A.

2. Déduisez la table de routage de A contenant pour chaque destination possible, le prochain nœud, le chemin complet et son coût.

3. On suppose que les liens A-B, puis D-E, puis B-C tombent en panne. A chaque fois la machine (ou les machines) qui détecte la panne émet un LSP contenant une distance infinie pour le lien en question. Représentez sous forme de graphe la connaissance que A a du réseau une fois que tout est stabilisé.

4. Le lien D-E est rétabli et le LSP correspondant est diffusé à tout le réseau. Calculez l'arbre couvrant pour A une fois que tout est stabilisé et déduisez-en la table de routage de A.

5. Ce fonctionnement est-il satisfaisant ? Justifiez ou proposez une solution.

Exercice 3 : Techniques d'accès (4 points)

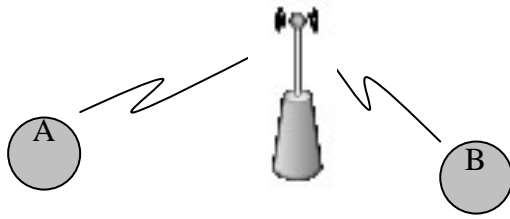
Une des fonctionnalités de la couche liaison dans un environnement TCP/IP est de « gérer » l'accès au canal partagé. Pour cette raison, le protocole Ethernet implémente le mécanisme CSMA/CD et bénéficie du fait que les stations peuvent écouter l'écho de leur transmission afin de détecter d'éventuelles collisions (2 transmissions simultanées).

1. Expliquez brièvement le principe du CSMA. Ce mécanisme, tout seul, est-il capable d'éliminer entièrement les collisions ?

Le mécanisme CSMA est aussi utilisé dans la couche liaison des réseaux sans fil avec le protocole IEEE 802.11 (wifi). La spécificité du sans fil est que les stations ne peuvent pas émettre et écouter leur transmission en même temps. Afin d'éviter les collisions, le protocole IEEE 802.11 nécessite l'échange d'un total de 4 messages (3 messages de contrôle + 1 trame de données) pour envoyer une seule trame de données. Ce mécanisme est appelé CSMA/CA (Collision Avoidance).

Considérons une trame de données à envoyer de taille 504 octets, 3 autres messages de contrôle de 48 octets chacun seront ajoutés.

2. En supposant que le temps d'attente entre chacun des messages est de 1 ms et que le temps de propagation sur le support sans fil est négligeable, calculez au niveau liaison le temps nécessaire pour envoyer entièrement la trame. Supposez un lien sans fil de 2 Mbit/s.



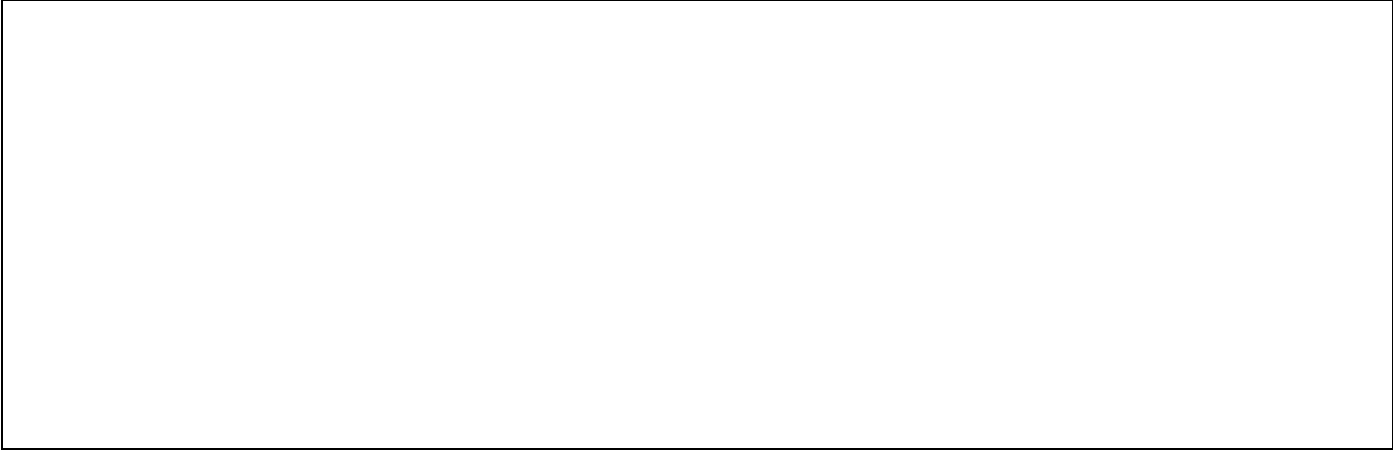
Ping et délai :

Nous voulons dans cette partie comparer le délai aller-retour dans un réseau sans fil à ce même délai dans un réseau filaire. Dans les deux cas, nous allons négliger les temps de traitement et de propagation et ne considérer que le temps de transmission.

3. Calculez le temps aller-retour d'un ping (écho request, écho reply) entre les machines A et B du réseau sans fil, sachant que la taille de la trame contenant le ping est de 104 octets et en gardant les mêmes hypothèses précédentes pour le réseau sans fil.

4. Calculez le délai si la technologie CSMA/CD (classique) est utilisée entre A et B. Dans ce cas, nous considérons des liens Ethernet de 10 Mbit/s et que le point d'accès est maintenant remplacé par un routeur dont le temps de traitement est négligeable. Que peut-on conclure ?

5. Que se passe-t-il, **dans le cas filaire seulement**, si avant d'envoyer le ping, les informations concernant l'adresse physique ne sont pas connues pour A sur le premier tronçon de la connexion ? Expliquez les échanges nécessaires afin de pouvoir pinger B.



Exercice 4 : Configuration IP (4 points)

Dans une salle machine, vous vous loguez sur une machine unix. Une étiquette vous indique l'adresse IP de cette machine : 131. 228.17.166.

1. Quel est le masque par défaut associé à cette adresse ? Pourquoi ?

2. Avec ce masque par défaut, quels sont l'adresse du réseau (*netid*) et l'identifiant de votre machine (*hostid*) ?

Vous souhaitez vérifier que l'adresse IP indiquée sur l'étiquette est correcte et connaître la valeur du masque utilisé, ainsi que l'adresse de diffusion sur ce réseau.

3. Quelle commande unix vous permet d'obtenir ces 3 informations ?

Le résultat de la commande ci-dessus vous indique que le masque utilisé ici est 255.255.255.240.

4. En supposant que l'on est parti du masque par défaut, combien de sous-réseaux ont pu au maximum être créés par cette subdivision ?

5. Quelle est l'adresse du réseau sur lequel votre machine est connectée ?

6. Quel est l'identifiant de votre machine sur ce réseau ?

7. Quelle est l'adresse de diffusion (*broadcast*) sur ce réseau ?

La machine sur laquelle vous êtes logué possède une seule carte réseau Ethernet. Pour accéder à Internet, les paquets passent par une passerelle.

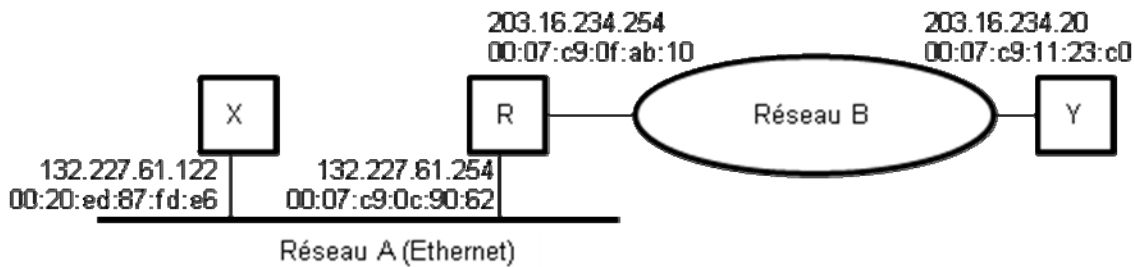
8. Quel est le nombre d'adresses IP possibles pour la passerelle ? Quelles sont-elles ?

9. Choisissez une adresse pour la passerelle et donnez la table de routage minimale de votre machine.

10. Quelle commande unix vous permet de vérifier que la table de routage donnée est conforme à votre réponse précédente ?

Exercice 5 : Codage/Décodage (4 points)

On considère 2 machines X et Y interconnectées via deux réseaux A et B et un routeur R.



Une trace a été obtenue sur le réseau A (Ethernet). De cette trace a été extraite la trame suivante (donnée sans préambule, ni CRC) :

```

00 07 e9 0c 90 62 00 20 ed 87 fd e6 08 00 45 00
00 28 b5 9f 00 00 40 06 0d ae 84 e3 3d 7a cb 10
ea 14 81 cf 00 50 52 40 18 64 00 00 00 00 50 02
ef 88 98 9e 00 00 00 00 00 00 00 00
  
```

1. Décodez la trame en délimitant ci-dessus soigneusement tous les champs protocolaires, en indiquant le nom de chaque champ et éventuellement sa valeur interprétée, puis répondez aux questions suivantes.

Quels sont (ou seront) les protocoles utilisés aux niveaux Réseau, Transport et Application, au cours de la communication ?

Quelle action de l'utilisateur et sur quelle machine a-t-elle pu déclencher l'envoi de cette trame ?

A quoi correspondent les 6 derniers octets de la trame ?

2. On suppose que le réseau B utilise un protocole d'accès dont la structure de trame est la même que celle d'Ethernet, à la différence que son champ de données ne peut excéder 36 octets de longueur.

Suite à l'émission de la trame précédente sur le réseau A, combien de trames seront ré-acheminées sur le réseau B ? Justifiez.

--

Donnez le codage hexadécimal des trames émises sur le réseau B (sans préambule, ni CRC), à raison d'un octet par case (les octets des champs « checksum » seront mis à XX).

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

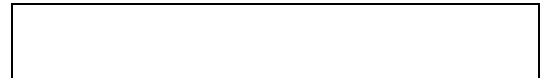
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--



Annexe

Structure d'une trame Ethernet

```

.....+--48bits--+--48bits--+16b+-- - - - +.....
.(Pré.) | adresse | adresse | type | données | (CRC).
.       | dest.   | source  |      |         |
.....+-----+-----+-----+-----+-----+

```

Quelques types : 0x0200 = XEROX PUP
0x0800 = DoD Internet
0x0806 = ARP
0x8035 = RARP

Structure d'un paquet IP

```

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

```

Ver = Version d'IP
IHL = Longueur de l'entête IP (en mots de 32 bits)
TOS = Type de service (zero généralement)
Fl (3 premiers bits) = Bits pour la fragmentation
* 1er = Reservé
* 2me = Ne pas fragmenter
* 3me = Fragment suivant existe
FO (13 bits suivants) = Position relative du fragment dans le datagramme initial, le déplacement étant exprimé en mots de 8 octets (seuls un datagramme complet ou un premier fragment peuvent avoir ce champ à 0)
TTL = Durée de vie restante

Quelques protocoles transportés :

- 1 = ICMP
- 2 = IGMP
- 4 = IP (encapsulation)
- 5 = Stream
- 6 = TCP
- 8 = EGP
- 11 = GLOUP
- 17 = UDP
- 36 = XTP
- 46 = RSVP

Structure d'un segment TCP

```

<-----32bits----->
<4b->      <-6bits-> <-----16bits----->
+-----+-----+-----+-----+-----+
| Port Source      | Port Destination |
+-----+-----+-----+-----+-----+
| Numéro de Séquence |
+-----+-----+-----+-----+-----+
| Numéro d'Acquittement |
+-----+-----+-----+-----+-----+
| THL |          | Flag | Taille Fenêtre |
+-----+-----+-----+-----+-----+
| Somme de ctrl (msg) | 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 = Données urgentes
- * 2me = Acquittement (ACK)
- * 3me = Données immédiates (Push)
- * 4me = Réinitialisation (Reset)
- * 5me = Synchronisation (SYN)
- * 6me = Fin

Options = suite d'options 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
4 Autorisation des acquittements sélectifs
8 Estampilles temporelles
L = un octet pour la taille totale de l'option
V = valeur de l'option (sur L-2 octets)

Services associés aux ports

ftp-data	20/tcp		
ftp	21/tcp		
ssh	22/tcp	ssh	22/udp
telnet	23/tcp		
smtp	25/tcp		
domain	53/tcp	domain	53/udp
tftp	69/udp		
finger	79/tcp		
www	80/tcp	www	80/udp
kerberos	88/tcp	kerberos	88/udp
pop-3	110/tcp	pop-3	110/udp
bgp	179/tcp		
		snmp	161/udp
		snmp-trap	162/udp
rtracerroute	3765/tcp		