

Introduction aux réseaux

Examen du 20/05/2016. Durée 2h.

Calculatrice autorisée, ainsi qu'une feuille A4 recto-verso manuscrite.

Les exercices sont indépendants. Vous pouvez les traiter dans l'ordre que vous souhaitez. Les réponses doivent être courtes, mais **bien justifiées**. Il y a beaucoup de questions, mais la plupart sont des reprises des TD ou du cours, et le barème se basera sur la proportion de questions validées dans le maximum d'exercices.

Exercice 1 : Analyse de trames

Pour cet exercice, consultez l'annexe pour la description des formats des PDU.

Un analyseur de protocoles, connecté à un réseau Ethernet permet de capturer le contenu des trames qui circulent sur le réseau. Les octets sont relevés sous forme hexadécimale. Ils représentent l'ensemble des octets des trames Ethernet sans les sept octets de préambule, ni l'octet de délimiteur de début de trame. Les 4 octets de CRC de fin de trame ne sont pas non plus affichés.

Une trame relevée au cours d'une session est la suivante :

```
00 25 84 DA 22 80 B8 8D 12 20 C4 B0 08 00 45 00 00 3C 85 1D
00 00 FF 11 BB 2F 82 BE 7B 4D C1 36 BC 21 C5 5A 00 35 00 28
01 57 9E 63 01 00 00 01 00 00 00 00 00 00 03 77 65 62 07 65
6E 73 69 6D 61 67 02 66 72 00 00 01 00 01
```

Question 1. *Expliquez le principe d'encapsulation qui permet d'analyser la signification des différents octets transmis.*

Question 2. *Extrayez l'en-tête Ethernet de cette trame : écrivez sur votre copie les octets correspondants.*

Question 3. *Montrez que le protocole réseau utilisé ici est IP. Extrayez son en-tête en expliquant la réponse. Quelle est la taille du paquet IP ?*

Question 4. *Quel est le protocole de la couche transport utilisé ici ? Extrayez son en-tête. Expliquez la réponse. Quelle est la taille du segment transport ? Est-ce normal connaissant la taille du paquet IP déterminée à la question précédente ?*

Question 5. *Dessinez l'empilement des couches avec les protocoles présents (et utilisés par la machine dans la trame) dans chaque couche.*

Exercice 2 : Echanges protocolaires

Un étudiant travaille sur son ordinateur, en naviguant sur le Web. On s'intéresse à la consultation suivante. Il saisit dans la barre d'adresse l'URL suivante :

<http://www.meteo.fr>

Il voit apparaître la page d'accueil du site de la météo.

Question 6. *(Scénario simple) Dessinez le diagramme temporel des échanges de PDU entre l'ordinateur de l'étudiant, le serveur DNS, et le site de la météo. Vous ferez figurer les échanges au niveau de la couche application, ainsi que les ouvertures et fermetures de connexion TCP.*

Question 7. Le scénario réel est un peu plus complexe. Après avoir saisi <http://www.meteo.fr>, il voit apparaître la page d'accueil du site de la météo, mais constate que sa barre d'adresse affiche une icône de cadenas suivie de l'adresse www.meteofrance.com/accueil. Pourtant, une interrogation du DNS par dig ou nslookup indique bien que www.meteo.fr est un site qui existe, n'a pas d'alias et a pour adresse IP 137.129.43.129. Expliquez ce qui s'est passé, comment l'adresse dans l'URL a changé. Proposez un diagramme temporel qui illustre ce scénario.

Exercice 3 : Performances : latence

Question 8. Rappelez, quelles sont les 4 sources de délai contribuant à la latence à chaque passage de routeur, et dans quel contexte cette source peut avoir un impact significatif.

Question 9. À l'instant 0, une machine A envoie un paquet de 1000 octets à une machine B, directement accessible (sans routeur) par un lien où les signaux se propagent à $2 \cdot 10^8$ m/s. Quand est-il reçu par B dans les cas suivants ?

- Distance(A,B) = 1km, débit liaison A-B = 10Mb/s
 - Distance(A,B) = 20m, débit liaison A-B = 1Gb/s
- NB : indiquez vos calculs, il ne suffit pas de donner la valeur finale.

Exercice 4 : Communication Radio

Un système radio utilise un canal fréquentiel de bande 6 MHz. La modulation utilisée est de type QAM avec un nombre de symboles égal à 4, 16, 32 ou 64. La rapidité de modulation est toujours de 5 Mbauds.

Question 10. Est-il possible réaliser la transmission numérique sans interférences entre symboles ? Si oui, comment ? (Précisez les caractéristiques des blocs à prévoir dans la chaîne de transmission).

Supposons qu'initialement on utilise une modulation QAM64, suffisante pour assurer un taux d'erreurs binaires correct (de l'ordre de 10^{-7}). Puis, suite à des interférences sur la liaison, la puissance de bruit augmente de 5 dB. Cf abaque en annexe sur les TEB.

Question 11. Quel taux d'erreurs binaires (TEB) a-t-on alors ? Expliquez pourquoi si l'on veut conserver la même qualité de transmission sur ce canal, il faut alors changer de modulation.

Question 12. Dites ce que valait au départ le débit binaire transmis. Si on décide de changer la modulation pour une modulation QAM16, quelle sera la nouvelle valeur du débit binaire ? Si l'on ne change pas la puissance émise, de combien de dB augmentera alors l'énergie du bit en réception ?

Question 13. Suffit-il de choisir une modulation QAM16 pour garantir à nouveau un taux d'erreurs binaires de 10^{-7} ? Si non, proposez une autre solution.

On décide de partager la liaison radio entre N utilisateurs différents. On hésite entre trois techniques d'accès différentes : de type CSMA, FDMA ou TDMA.

Question 14. Si l'on veut garantir à l'utilisateur que la ressource radio lui sera toujours disponible, il y a une de ces techniques à éviter. Laquelle et pourquoi ?

Exercice 5 : Adresses IP

Une société missionne un stagiaire Ensimag pour faire évoluer l'infrastructure de son système d'information.

1. Afin de satisfaire les besoins de la Direction en matière de connectivité mobile, il faut passer de 13 à 72 adresses IP en WiFi.
2. Au cours des 2 prochaines années, le Département Stagiaires et Intérimaires va voir passer ses besoins de 29 à plus d'une centaine de postes de travail.
3. Le Département de gestion des stocks doit se doter d'un système d'archivage redondant et sécurisé de 16 systèmes de stockage (chacun doté d'une adresse IP).
4. Le Département Comptabilité et Facturation va évoluer pour intégrer un cluster de calcul de 26 machines.

Le stagiaire doit découper un bloc d'adresses privées afin de configurer les sous-réseaux derrière la passerelle. Chaque sous-réseau est raccordé par une passerelle au reste de l'infrastructure de la société. Par convention, chacune de ces passerelles prend la première adresse du sous-réseau.

Question 15. *Trouvez les besoins en adresses IP de chaque sous-réseau.*

Question 16. *Quel bloc d'adresses privées vous semble le plus adapté entre 10.0.0.0/24 et 172.16.0.0/20?*

Question 17. *Procédez au découpage du bloc d'adresses privées sélectionné et assignez les groupes d'adresses aux différents sous-réseaux, en précisant le masque de chacun des sous-réseaux.*

Exercice 6 : Cryptographie

Un utilisateur possède des comptes sur les machines `pc.epfl.ch` et `mac.epfl.ch`. Sur chaque machine, il a généré une paire de clés pour l'authentification ssh : `id_rsa` et `id_rsa.pub`. Son répertoire `.ssh` sur la machine `pc.epfl.ch` contient des fichiers avec des clés publiques. Les empreintes (empreintes = fingerprint) de ces clés sont les suivantes :

`known_hosts:`

1024 c6:87:44:98:b6:b8:6c:d1:f8:17:c9:75:44:5d:71:76 mac.epfl.ch

`authorized_keys:`

1024 8e:e8:14:8e:ca:03:ce:e5:75:1b:3c:0c:ae:b4:64:f9

`id_rsa.pub:`

1024 e3:c8:64:89:d7:46:7e:2d:de:72:0e:b4:bb:03:1a:a5

De même, les empreintes des clés publiques sur la machine `mac.epfl.ch` sont les suivantes :

`known_hosts:` (vide)

`authorized_keys:`

1024 93:8c:21:7d:3b:b9:92:e7:d6:dc:33:d5:42:7e:9b:cd

`id_rsa.pub:`

1024 8e:e8:14:8e:ca:03:ce:e5:75:1b:3c:0c:ae:b4:64:f9

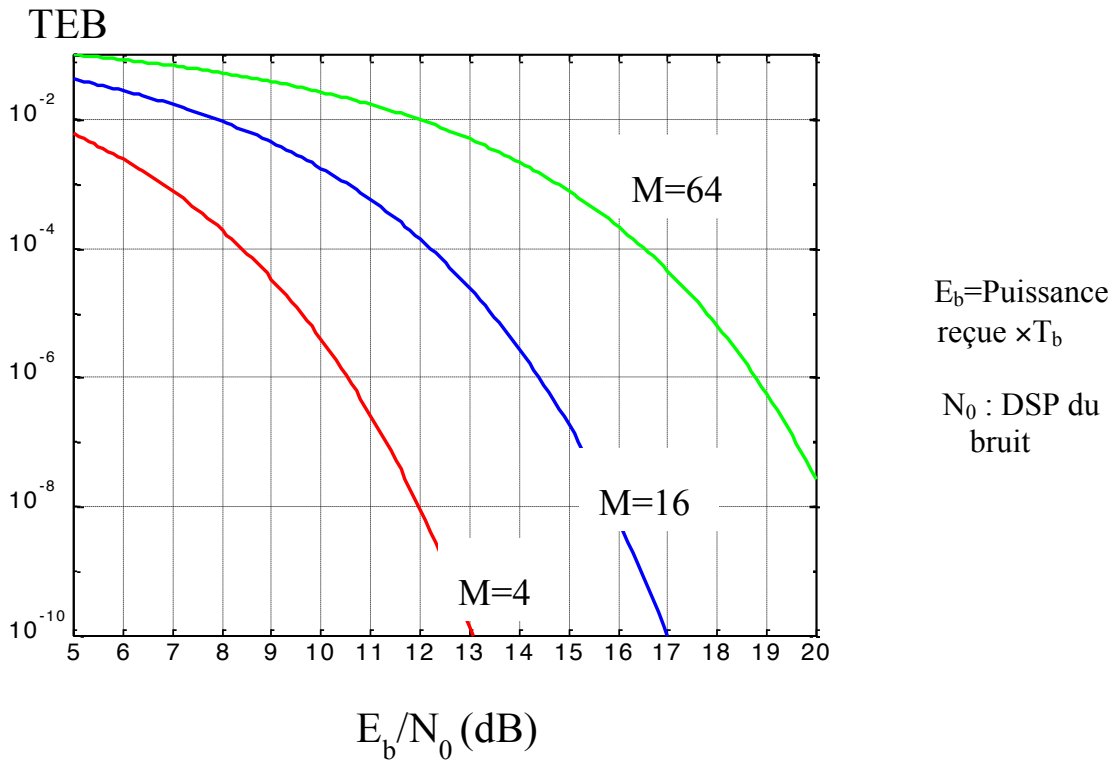
Question 18. *Peut-il se connecter de `pc.epfl.ch` à `mac.epfl.ch` sans donner le mot de passe ?*

Question 19. *Même question de `mac.epfl.ch` à `pc.epfl.ch` ?*

Question 20. *Que va-t-il se passer s'il exécute la commande `ssh pc.epfl.ch` sur `mac.epfl.ch` ?*

Annexe :

Courbes de performance des modulations QAM-M :



Protocoles réseaux

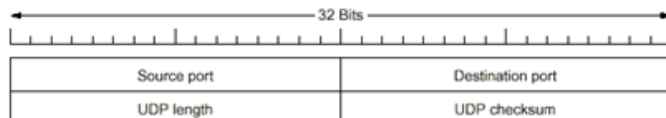
Format d'une trame Ethernet

7 fois 10101010	10101011	adresse destination	adresse source	type de protocole réseau	données / remplissage	FCS (CRC)
7 octets	1	6	6	2	0 à 1500 / 0 à 46	4

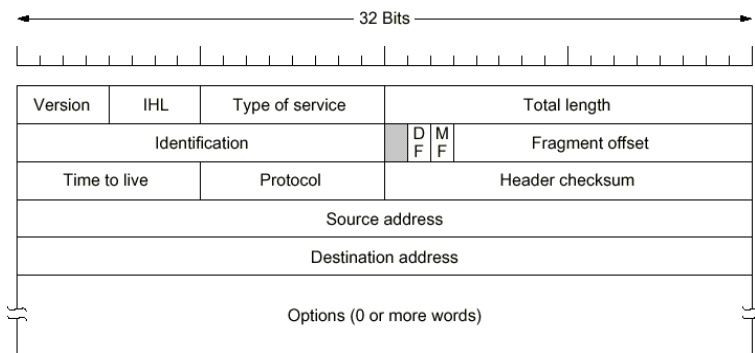
Signification du champ 'type de protocole réseau' :

0x6000 - DEC
0x0609 - DEC
0x0600 - XNS
0x0800 - IPv4
0x0806 - ARP
0x8019 - Domain
0x8035 - RARP
0x809B - AppleTalk
0x86DD - IPv6

Format de l'en-tête d'un segment UDP

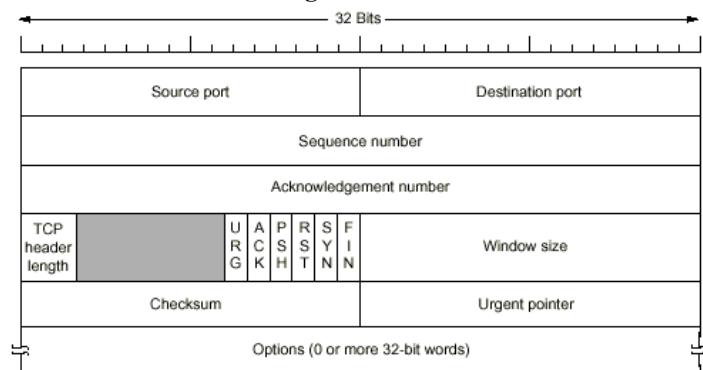


Format de l'en-tête d'un paquet IP



Code (déc)	Abréviation	Nom du protocole	Reference
0		Reserved	
1	ICMP	Internet Control Message	[RFC792]
2	IGMP	Internet Group Management	[RFC1112]
3	GGP	Gateway-to-Gateway	[RFC823]
4	IP	IP in IP (encapsulation)	
5	ST	Stream	[RFC1190]
6	TCP	Transmission Control	[RFC793]
7	UCL	UCL	
8	EGP	Exterior Gateway Protocol	[RFC888]
9	IGP	any private interior gateway	
10	BBN-RCC-MON	BBN RCC Monitoring	
11	NVP-II	Network Voice Protocol	[RFC741]
12	PUP	PUP	
13	ARGUS	ARGUS	
14	EMCON	EMCON	
15	XNET	Cross Net Debugger	
16	CHAOS	Chaos	
17	UDP	User Datagram	[RFC768]

Format de l'en-tête d'un segment TCP



Application	N° de Port (décimal)	Type	Commentaire
ICMP	7	TCP/UDP	Commandes Ping
Netstat	15	TCP/UDP	Etat du réseau
FTP	21	TCP	Transfert de fichiers
SSH	22	TCP/UDP	SSH Remote Login Protocol
Telnet	23	TCP	Connexion via terminal réseau
SMTP	25	TCP	Envoi de courrier
DNS	53	TCP/UDP	Serveurs de noms de domaine
HTTP	80	TCP	Serveur Web
Pop3	110	TCP	Réception de courrier
nntp	119	TCP	Service de news
ntp	123	UDP	Protocole temps réseau
nbname	137	TCP/UDP	Service de Nom Netbios
netbios-ssn	139	TCP/UDP	Service de Session Netbios
imap	143	TCP/UDP	Protocole d'accès messagerie Internet
SNMP	161	UDP	Administration de réseau