Exercice 1: Questions modèle OSI – Modèle TCP/IP

1- Qu'est-ce que l'ISO ?
2- Que signifie OSI ? Pour quelles raisons à t'on créer ce modèle ? Quels sont ses avantages ?
3- Combien de couches comporte ce modèle. Donner le nom et la fonction de chacune des couches.
4- Que signifie communication d'égal à égal ?
5- Qu'est-ce que l'encapsulation ?
6- Qu'est-ce qu'un "PDU" ?
7- Comment se nomme les PDU des couches 1, 2, 3, 4, 5, 6 et 7.
8- Quels PDU circulent dans un réseau local ?, dans un réseau de type Intranet ou Internet?
9- Qu'est-ce qu'un protocole ?
10- Comment se nomme le modèle utilisé par l'Internet ?
11- Décrire chacune des couches de ce modèle ?
12- Qui est à l'initiative de la création des réseaux TCP/IP ?
13- Quelle est sa caractéristique principale ? Expliquer !
14- Combien de couche comporte le modèle TCP/IP ? Donner le nom et la fonction de chacune des couches.
15- Expliquer la différence entre un protocole orienté connexion et un autre non orienté connexion ?
16- Comment se nomme une communication faisant appel :
17- A un circuit logique temporaire ?
18- A un circuit logique non temporaire ?
a. Donner un exemple de communication à commutation de circuit.
b. Quelles différences majeures distinguent TCP/IP du modèle OSI ?

Exercice 2 : Modèle OSI

1- Définissez de manière succincte les termes suivants : Couche, Système, Entité, Protocole, Service.
Quelques indications :
Pour simplifier la description d'un système complexe (exemple Os Réseau), on introduit la notion de couche. Une couche peut être logicielle ou matérielle.

Exemple OSI :
La couche (N) offre des services à la couche (N+1)
La couche (N) utilise les services de la couche (N-1)
Un protocole de niveau N précise comment communiquent des entités de systèmes différents pour une même couche N.

- Donnez une description des différentes couches du modèle OSI.

Couches	Descriptions
Application	La couche Application ne définit pas des applications en soi, mais le moyen d'accéder à l'environnement OSI La structure de la couche Application détermine comment différentes applications vont être organisées pour utiliser des modules OSI communs
Présentation	S'intéresse à la sémantique des données échangées **Offre des services** * **De codage et décodage de l'information** – Pour permettre la communication entre machines utilisant des modes de représentation différents (codes ASCII et EBCDIC) – Basés sur la syntaxe abstraite ASN.1 définit dans les norme ISO 8824 et avis X.208 de l'UIT * **De compression de l'information** * **De chiffrement de l'information** (de bout en bout)

	– Par des méthodes de cryptage à clef publique ou privée – Pour assurer la confidentialité, l'authentification et la non répudiation des données
Session	Offre des services à valeurs ajoutées aux couches supérieures **Libération ordonnée de session** **Gestion du dialogue** (pour des liaisons fonctionnant à l'alternat) **Synchronisation des échanges** (pour gérer les erreurs de niveau supérieur) Gestion des activités ou transactions
Transport	La couche Transport = Interface entre : Couches basses (transmission de l'information) et couches hautes (traitement de l'information) . **Effectue des contrôles supplémentaires à ceux déjà effectués par le couche Liaison, mais ces contrôles sont effectués de bout en bout**
Réseau	Principales fonctions apportées : **Fonctions d'adressage** (systèmes d'adressage hiérarchiques où deux entités voisines ont des adresses comparables) **Fonctions de routage** (pour déterminer les chemins à suivre pour interconnecter deux sous-réseaux ou entités)
Liaison	Elle permet la transmission de données de manière fiable entre deux entités connectées directement (au niveau physique) A l'émission, les données sont assemblées en trames pour être échangées A la réception, les frontières entre trames envoyées par la couche Physique doivent être détectées **Deux types de fonction sont principalement apportés :** - des fonctions de contrôle d'erreurs et de contrôle de flux (pour veiller à la bonne transmission de l'information) - des fonctions de contrôle d'accès au support (quand un même support est partagé entre plusieurs stations)
Physique	permet la transmission de bits sur un circuit de communication fournit les moyens mécaniques, électriques et fonctionnels pour le maintien et l'utilisation des connexions physiques définit à la fois : l-es supports de transmission (câbles et connecteurs) les modes de transmission de l'information (en bande de base et par modulation)

- Dans quelles couches sont spécifiés les protocoles[1]: CSMA/CD, DNS, ARP, ICMP, ASN1 ?

- Quels sont les rôles des protocoles cités ci-dessus ?

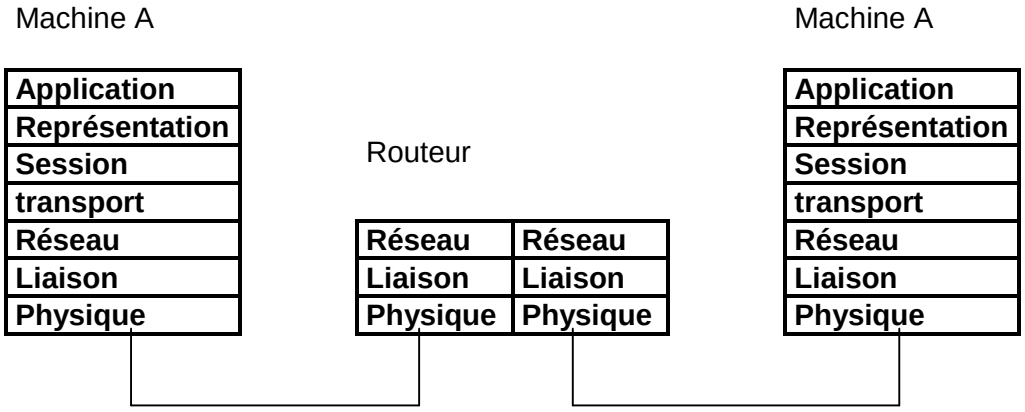
Couche	Protocole	Rôles
Application	DNS	Système hiérarchique Résolution @IP <> nom
Présentation	ASN1	Voir exercice précédant
Session		
transport		
Réseau	ICMP, ARP	ICMP : diagnostique ARP résolution AIP en @MAC
Liaison	CSMA/CD	*Carrier sense multiple access collision detect Détection de porteuse avec accès multiple. Mécanisme d'accès aux médias par lequel les unités qui sont prêtes à transmettre des données vérifient d'abord le canal afin de détecter une porteuse. Si aucune porteuse n'est détectée*

[1] Par rapport à OSI

		pendant un délai donné, l'unité peut transmettre. Si deux unités transmettent simultanément, une collision se produit et elle est détectée par toutes les unités touchées. Cette collision retarde ensuite toute nouvelle transmission par ces unités pour une période de temps aléatoire. L'accès CSMA/CD est utilisé par les protocoles Ethernet et IEEE 802.3.
Physique		

Exercice 3 : OSI – Routage

On considère qu'une application de la machine A dialogue avec son homologue de la machine C.
Une machine B, un routeur, relie les réseaux respectifs des machines A et C.
Dessiner et définir les piles de protocoles du modèle OSI mises en jeu sur A, B et C.



Exercice 4 : Mode connecté et non connecté – exemples

Une relation à travers un réseau WAN se distingue par le type de relation mise en œuvre. Le tableau ci-dessous compare ces deux modes, veuillez le reproduire et le compléter.

	Mode non connecté mode datagramme	**Mode orienté connexion** mode connecté
Phase de mise en relation	non	oui
Garantie du séquencement	non	oui
Réservation de ressources	non	oui
Contrôle de flux	non	oui
Contrôle et reprise sur erreur	non	oui
Optimisation des ressources	oui	non
Complexité au niveau du réseau	non	oui
Complexité au niveau des systèmes d'extrémité	oui	non
Possibilité de redevance au volume	non	oui
Possibilité de redevance forfaitaire	oui	oui
Exemples de protocole : Réponse attendues	**IP**, LLC1, **UDP**	HDLC, FR, ATM, **X25** **TCP**, TP0 à TP4, SNA

Exercice 4 : Réseau Ethernet.

1. Expliquez le principe de communication **CSMA/CD** [2] qui régit un réseau Ethernet.
2. Décrivez le but et le mode de fonctionnement du protocole ARP lorsqu'il est utilisé sur un réseau local de type Ethernet.
3. Soit un réseau local Ethernet contenant 3 serveurs et 50 postes tous interconnectés via une pile de hubs. Proposez une solution pour améliorer les performances du réseau en expliquant pourquoi votre solution est meilleure que la situation initiale.

[2] Carrier Sense Multiple Access with Collision Detect

Exercice 5: Fragmentation IP.

1. Pourquoi un routeur IP fragmente-t-il un datagramme?

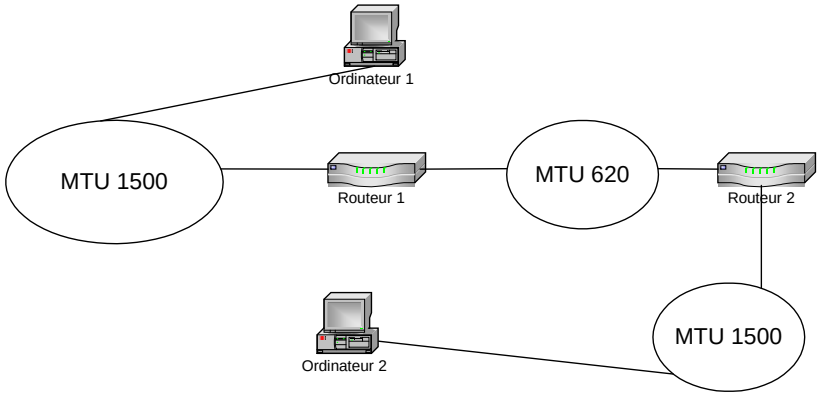
La taille d'un datagramme maximale est de 65535 octets. Cette valeur n'est jamais atteinte car les réseaux n'ont pas une capacité suffisante pour envoyer de si gros paquets.
Les réseaux sur Internet utilisent différentes technologies ⇒ la taille maximale d'un datagramme varie suivant le type de réseau.
La taille maximale d'une trame est appelée ***MTU*** **(Maximum Transfer Unit**), elle entraînera la fragmentation du datagramme si celui-ci a une taille plus importante que le MTU du réseau.

Type de réseau	MTU (en octets)
Arpanet	**1000**
Ethernet	**1500**
FDDI	**4470**

Le routeur envoie les fragments de manière indépendante et réencapsulé (il ajoute un en-tête à chaque fragment) pour tenir compte de la nouvelle taille du fragment, et ajoute des informations afin que la machine de destination puisse réassembler les fragments dans le bon ordre.

Chaque datagramme possède plusieurs champs permettant leur réassemblage:
- **champ déplacement de fragment**: champ permettant de connaître la position du début du fragment dans le datagramme initial
- **champ identification**: numéro attribué à chaque fragment afin de permettre leur réassemblage dans le bon ordre
- **champ longueur total**: recalculé pour chaque fragments
- **champ drapeau**: composé de trois bits:
  - Le premier non utilisé
  - Le second (appelé **DF**: *Don't Fragment*) indique si le datagramme peut être fragmenté ou non. Si jamais un datagramme a ce bit positionné à un et que le routeur ne peut pas l'acheminer sans le fragmenter, alors le datagramme est rejeté avec un message d'erreur
  - Le dernier (appelé **MF**: *More Fragments*, en français *Fragments à suivre*) indique si le datagramme est un fragment de donnée (1). Si l'indicateur est à zéro, cela indique que le fragment est le dernier (donc que le routeur devrait être en possession de tous les fragments précédents) ou bien que le datagramme n'a pas fait l'objet d'une fragmentation

2. À l'aide d'un exemple, expliquez le processus de fragmentation IP en citant les champs du datagramme nécessaires à cette fragmentation.



La fragmentation se situe au niveau d'un routeur qui reçoit des datagrammes issus d'un réseau à grand MTU et qui doit les réexpédier vers un réseau à plus petit MTU. Dans cet exemple, si l'ordinateur 1, reliée à un réseau Ethernet, envoie un datagramme de 1400 octets à destination de l'ordinateur 2, reliée également à un réseau Ethernet, le routeur 1 fragmentera ce datagramme de la manière suivante.

La taille d'un fragment est choisie la plus grande possible tout en étant un multiple de 8 octets.

- Un datagramme fragmenté n'est réassemblé qu'à destination finale.
- Chaque fragment est routé indépendamment des autres.
- Le destinataire final recevant le premier fragment arme un temporisateur de réassemblage. Passé ce délai, si tous les fragments ne sont pas arrivés il détruit les fragments reçus et ne traite pas le datagramme.

Exercice supplémentaire :

1- Soit un hôte dont le logiciel IP doit envoyer un datagramme sans option contenant 6 000 octets de données à travers un réseau de MTU 1 800 : Fragmenter le datagramme et indiquer ces mêmes champs pour tous les fragments obtenus.

2- Le premier fragment et le troisième sont arrivés à un routeur qui doit les réexpédier par un réseau de MTU 1000. Indiquer les champs précédents pour les fragments fabriqués par ce routeur.

Réponse 1

	Octets		
Messages	6000		
MTU	1800		
En tete IP	20	Divibles / 8	
Donnees utiles	**1780**	**1776**	4
	222,5		

En tete IP taille en octets		Datagramme en octets		
20		6000		
Taille totale du datagramme	identification	DF	MF	offset
6020	12345	0	0	0

Nbre de paquets	Partie entiere	Reste en octets
3,378378378	3	**672**

Paquets transmis :

	En tete IP taille en octets		Datagramme en octets		
Paquet1	20		1776		
	Taille totale du datagramme	identification	DF	MF	offset
	1796	12345	0	1	0
Paquet2	En tete IP taille en octets		Datagramme en octets		
	20		1776		
	Taille totale du datagramme	identification	DF	MF	offset
	1796	12345	0	1	222
Paquet3	En tete IP taille en octets		Datagramme en octets		
	20		1776		
	Taille totale du datagramme	identification	DF	MF	offset
	1796	12345	0	1	444
Paquet3	En tete IP taille en octets		Datagramme en octets		
	20		672		
	Taille totale du datagramme	identification	DF	MF	offset
	692	12345	0	0	666

Exercice 6: Adressage IP.

1. Sur un réseau IP de classe B, donnez :

- la structure binaire précise,

2. Une station est configurée avec l'adresse IP privée 172.168.14.100 et le masque de réseau est 255.255.255.240.

Commentez le terme d'adresse IP privée. *Adresses privées non routables, utilisées pour palier à une insuffisance de l'adressage IPV4.*

L'Autorité d'Affectation de Numéros sur Internet (IANA) a réservé 3 blocs dans l'espace d'adressage pour des réseaux internes :

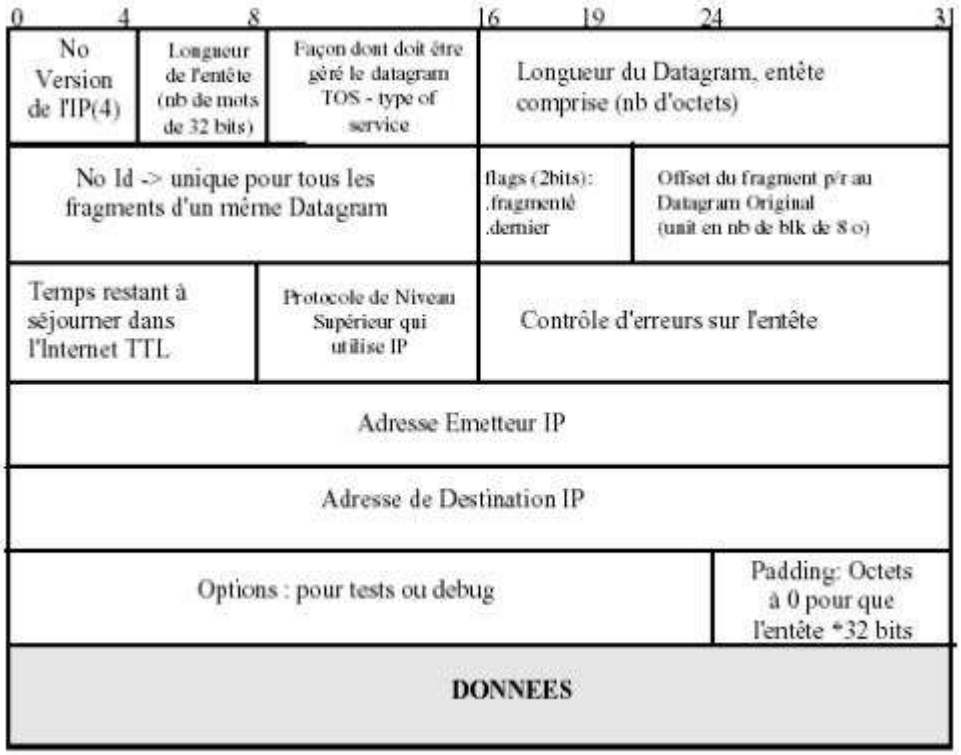
	DEBUT	FIN
Classe A	10.0.0.0	10.255.255.255
Classe B	172.16.0.0	172.31.255.255
Classe C	192.168.0.0	192.168.255.255

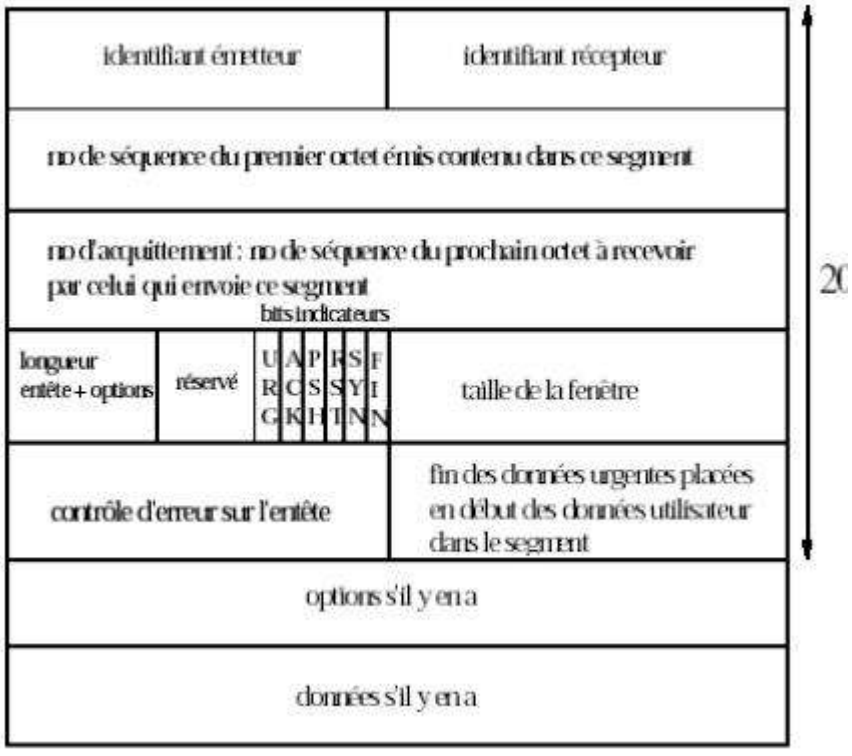
- Donnez l'adresse du sous-réseau auquel appartient la station et l'adresse de diffusion de ce sous-réseau.

3. Une entreprise souhaite organiser son réseau en le découpant en 15 sous-réseaux distincts, tous

bâtis à partir de son réseau de classe B (172.16.0.0 /16) . Comment doit-elle procéder au niveau de l'adressage IP ?

Exercice 7 : La couche Transport (éléments de correction)
On donne la structure de l'entête IP et la structure de l'entête TCP.





Trace d'une communication point à point prélevée par Ethereal (voir page suivante) :
A votre avis, à quoi correspondent les étiquettes TCP et TELNET ?
Combien y a-t-il d'encapsulations successives ?
Déterminer le début du paquet IPv4.
Déterminer la fin de l'entête du paquet IPv4.
Déterminer la fin de l'entête TCP.

Frame 6 (78 on wire, 78 captured)
Arrival Time: Mar 12, 2003 11:45:36.312497000
Time delta from previous packet: 0.563194000 seconds
Time relative to first packet: 0.657684000 seconds
Frame Number: 6
Packet Length: 78 bytes
Capture Length: 78 bytes

Ethernet II

Destination: **00:03:47:9c:fb:0d** (Intel_9c:fb:0d)
Source: 00:a0:c9:df:31:dd (INTEL_df:31:dd)
Type: IP (0x0800)

Internet Protocol, Src Addr: 192.168.14.100 (192.168.14.100), Dst Addr: 192.168.14.105 (192.168.14.105)

Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 64
Identification: 0x047f
Flags: 0x04
.1.. = Don't fragment: Set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 64
Protocol: TCP (0x06)
Header checksum: 0x981b (correct)
Source: 192.168.14.100 (192.168.14.100)
Destination: 192.168.14.105 (192.168.14.105)

Transmission Control Protocol, Src Port: telnet (23), Dst Port: 32787 (32787), Seq: 190238143, Ack: 190969207, Len: 12

Source port: telnet (23)
Destination port: 32787 (32787)
Sequence number: 190238143
Next sequence number: 190238155
Acknowledgement number: 190969207
Header length: 32 bytes
Flags: 0x0018 (PSH, ACK)
0... .... = Congestion Window Reduced (CWR): Not set
.0.. .... = ECN-Echo: Not set
..0. .... = Urgent: Not set
...1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
.... ..0. = Syn: Not set
....0 = Fin: Not set
Window size: 32120
Checksum: 0x**0ea0** (correct)
Options: (12 bytes)
NOP
NOP
Time stamp: tsval 698836, tsecr 296746888

Telnet----------

Command: Do Terminal Type
Command: Do Terminal Speed
Command: Do X Display Location
Command: Do New Environment Option

```
0000  00 03 47 9c fb 0d 00 a0 c9 df 31 dd 08 00 45 00   ..G.....1...E.
0010  00 40 04 7f 40 00 40 06 98 1b c0 a8 0e 64 c0 a8   .@..@.@......d..
0020  0e 69 00 17 80 13 0b 56 cd bf 0b 61 f5 77 80 18   .i.....V...a.w..
0030  7d 78 0e a0 00 00 01 01 08 0a 00 0a a9 d4 11 af   }x..............
0040  ff 88 ff fd 18 ff fd 20 ff fd 23 ff fd 27         ....... ..#..'
```

Exercice 8 : Segmentation de réseau TCP/IP

L'un des établissements d'une entreprise utilise la plage d'adresse 10.0.0.0 de la classe A. Considérons quatre machines de cet établissement dont les noms et adresses sont donnés ci-dessous :

Nom	Adresse IP	Adresse MAC
User1.Entreprise.com	10.99.43.27	00-90-27-55-74-35
User2.Entreprise.com	10.163.12.254	00-90-27-55-74-36
User3.Entreprise.com	10.189.12.27	00-90-27-55-74-37
User4.Entreprise.com	10.126.43.254	00-90-27-55-74-38

a) Quel est le NetID de ce plan d'adressage ?
En classe A le NetID est exprimé sur 1 octect, soit 10 pour le premier octet

b) Quel est le nombre de bit nécessaires pour réaliser deux sous-réseaux (SubNetID) tels que User1 et User4 appartiennent au même sous réseaux et que User2 et User3 appartiennent à un autre sous-réseau. On rappelle que les bits du NetID et du SubNetID doivent être contigus. Donnez le masque correspondant.
Pour distinguer le nombre de bits nécessaires il suffit d'examiner la valeur binaire du 1er octet du Host_ID, si cela est insuffisant du second.... jusqu'à trouver la combinaison binaire qui réponde au problème posé.

Station	octet 1 du HostID	Sous-réseau
99	**01 100011**	**SR1**
163	**10 100011**	**SR2**
189	**10 111101**	**SR2**
126	**01 111110**	**SR1**

L'examen du tableau ci-dessus montre que seuls deux bits sont nécessaires pour distinguer dans le plan d'adressage donné les 2 sous-réseaux.
Le masque de sous réseau correspondant est : 255.192.0.0

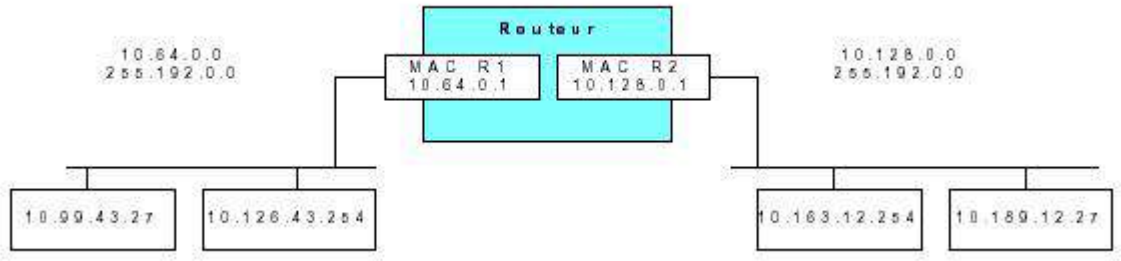
c) Quel est le nombre de bits minimum et nécessaire pour qu'aucune des machines n'appartiennent au même sous réseau. Donnez le masque correspondant.
La plus petite combinaison binaire pour distinguer 4 sous-réseaux distincts dans les adresses données est de 4. Le masque de sous-réseau est alors : 255.240.0.0

d) Pour permettre la communication entre les deux sous-réseaux de la question b, on relie les brins Ethernet de ces deux sous-réseaux par un routeur configuré en proxy ARP (Celui-ci répond en lieu et place des stations connectées sur ses autres liens). Si on affecte à chaque interface LAN de ce routeur la première adresse disponible (NetHost = 1), quelles sont les adresses affectées. Représentez l'ensemble par un schéma.

L'adresse réseau de chacun des deux sous-réseaux constitués est :
10D.01000000B.0D.0D
10D.10000000B.0D.0D

Notation provisoire utilisée pour indiquer comment sont déterminées les adresses réseaux : D signifie Décimal, B binaire, soit en notation décimale pointée :
10.64.0.0 masque 255.192.0.0
10.128.0.0 masque 255.192.0.0

Le schéma suivant représente le réseau obtenu :



e) Toutes les stations viennent de communiquer entre elles, quel est le contenu de la table ARP de la station de User1 ? Pour cette question vous affecterez des adresses MAC fictives à chaque interface du routeur : MAC R1 et MAC R2.

La table ARP de la station de User1 est :

@IP	**@MAC**
10.126.43.254	MAC_4
10.64.0.1	MAC_R1

f) L'établissement envisage de raccorder son réseau à Internet. Est ce possible en l'état, quelle est la difficulté et quelle solution proposeriez-vous ?
L'entreprise utilise l'adresse 10 qui est une adresse non routable sur Internet. Elle devra faire la demande d'affectation d'adresses officielles. Si elle ne veut pas avoir à revoir la configuration de toutes ses machines, elle devra mettre en œuvre le NAT (translateur d'adresses pour avoir accès à Internet).

Exercice 9 : Masque de sous-réseau

Deux réseaux (A et B) utilisent le protocole TCP/IP, ils sont reliés via un routeur.
L'entreprise a défini le masque de sous-réseau : 255.255.0.0. Un utilisateur du réseau A sur la machine 100.64.0.102 se plaint de ne pouvoir joindre un correspondant d'adresse 100.64.45.102 du réseau B. Expliquez pourquoi ?
ATTENTION : la notion de classe d'adressage apparaît pour certains comme un concept obsolète (CDIR), cependant la ,plupart des systèmes de configuration reconnaissent encore les classes.

Solution :
Rappelons qu'IP utilise 3 types d'adressage (Classe A, B, C). Les premiers bits du premier octet identifient la classe :
− les valeurs 1 à 126 correspondent à un adressage de classe A,
− les valeurs 128 à 191 correspondent à un adressage de classe B,
− les valeurs 192 à 223 correspondent à un adressage de classe C.

Dans notre cas, le réseau utilise un adressage de classe A, le second octet correspond donc au sous-réseau et les octets suivants à l'adressage de la station.
Les deux stations du réseau représenté figure 20.59 ne peuvent correspondre puisqu'elles sont, vis-à-vis du masque de sous-réseau sur le même réseau.

Figure 20.59 – Réseau défaillant.

Soit il s'agit d'une erreur de configuration d'une des stations qu'il suffit alors de corriger, soit d'une erreur dans la définition du masque de sous-réseau qui porté à 24 bits distinguerait alors deux sous-réseaux distincts.

Compléments sur l'adressage :

- A quel usage l'adresse 127.x.x.x est réservée ?

Cette adresse ne peut être attribuée, elle désigne la machine elle-même. Tout paquet émis à cette adresse revient à l'émetteur sans transiter sur le réseau (adresse de test).

- L'adresse 0.0.0.0 n'est pas attribuée, elle est utilisée pendant certaines procédures d'initialisation.

10 Masque de sous-réseau

Une entreprise à succursale multiple utilise l'adresse IP 196.179.110.0. Pour une gestion plus fine de ses sous-réseaux, le responsable informatique désire pouvoir affecter une adresse IP propre à chaque sous-réseau des 10 succursales.

1) De quelle classe d'adressage s'agit-il ?
2) Donner et expliquez la valeur du masque de sous-réseau correspondant à ce besoin.
3) Combien de machines chaque sous-réseau pourra-t-il comporter et pourquoi ?
4) Quelle est l'adresse de broadcast du sous-réseau 3 (expliquez) ?

Solution :

1) & 2)

Comme on doit pouvoir adresser 10 sous-réseaux, il faut donc 10 adresses IP dérivées de l'adresse initiale. La valeur décimale 10 se code par 1010 en binaire, il faut donc disposer de 4 bits. Le masque de sous-réseau à construire est donc :
11111111.11111111.11111111.11110000 soit encore :
255.255.255.240

La valeur binaire du premier octet permet de définir la classe d'adressage : 196D = 1100 0100B, soit une classe C (110)

3)

Compte tenu des bits affectés au masque de sous-réseau, il reste 4 bits pour identifier les machines, la valeur 0 représentant le sous-réseau lui-même, la valeur tout à 1 représente l'adresse de broadcast, chaque sous-réseau ne pourra comporter que 14 machines au maximum.

4)

L'adresse de broadcast correspond à tous les bits du champ Host_ID à 1, soit pour le sous-réseau 3, en ne considérant que le dernier octet : 0011 1111 où le premier quartet désigne le sous-réseau 3, le second désignant le Host_ID a tous ses bits à 1. Ce qui, pour cet octet, correspond en décimal à 63, soit l'adresse de diffusion : 196.179.110.63

Attention : Il n'y a pas ambiguïté dans l'affectation de la valeur du sous-réseau, la valeur 0 n'étant jamais utilisée pour des raisons de compatibilité. En effet, une vieille version de UNIX considère le champ à zéro comme étant l'adresse de diffusion (UNIX BSD).

11 Trace TCP/IP

La trace reproduite ci-dessous a été réalisée sur réseau de type Ethernet. On vous demande d'analyser celle-ci et de fournir toutes les informations relatives au protocole utilisé.
Dans la deuxième trame proposée, ne commentez que les parties intéressantes vis-à-vis de ce qui a déjà été commenté dans la première trame.

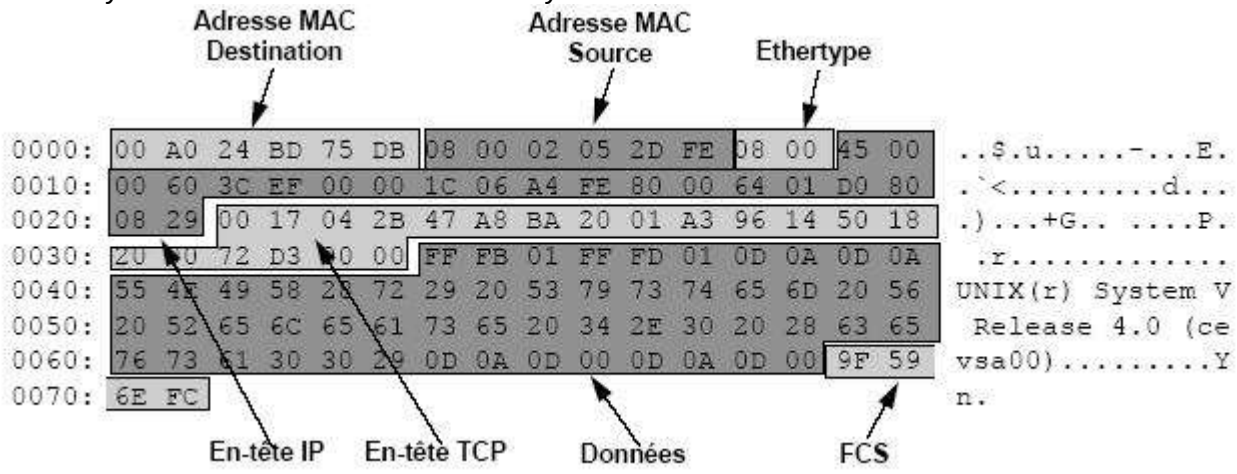
```
Captured at: +00:03.934
Length: 114 Status: Ok
OFFST DATA ASCII
0000: 00 A0 24 BD 75 DB 08 00 02 05 2D FE 08 00 45 00 ..$.u.....-...E.
0010: 00 60 3C EF 00 00 1C 06 A4 FE 80 00 64 01 D0 80 .‘<.........d...
0020: 08 29 00 17 04 2B 47 A8 BA 20 01 A3 96 14 50 18 .)...+G.. ....P.
0030: 20 00 72 D3 00 00 FF FB 01 FF FD 01 0D 0A 0D 0A .r..............
0040: 55 4E 49 58 28 72 29 20 53 79 73 74 65 6D 20 56 UNIX(r) System V
0050: 20 52 65 6C 65 61 73 65 20 34 2E 30 20 28 63 65 Release 4.0 (ce
0060: 76 73 61 30 30 29 0D 0A 0D 00 0D 0A 0D 00 9F 59 vsa00).........Y
0070: 6E FC n.
Captured at: +00:04.771
Length: 64 Status: Ok
OFFST DATA ASCII
0000: 00 A0 24 BD 75 DB 08 00 02 05 2D FE 08 00 45 00 ..$.u.....-...E.
0010: 00 29 3C F2 00 00 1C 06 A5 32 80 00 64 01 D0 80 .)<......3..d...
0020: 08 29 00 17 04 2B 47 A8 BA 62 01 A3 96 1B 50 18 .)...+G..b....P.
0030: 20 00 D2 14 00 00 63 00 00 08 00 00 69 55 A1 FF .....c.....iU..
```

Solution :

Remarque :
La trace proposée est une reproduction d'une trace obtenue avec un analyseur de protocole Ethernet. L'analyseur extrait le préambule, les fanions et ne présente que les données utiles. Le contenu de la trame en hexadécimal est interprété (codage ASCII), ce qui facilite le travail d'analyse.
En effet, le décodage du champ données laisse clairement apparaître son contenu : UNIX® System V... De ce fait, l'on sait déjà que l'on peut s'attendre à ce que le protocole réseau utilisé soit IP du DoD. La valeur des octets 13 et 14 (Ethertype ou type de protocole) confirment ces dires.
Le protocole supérieur est TCP/IP (valeur 0x0800).

Méthode d'analyse

A partir de la structure du bloc de données rappelée dans l'énoncé. On découpe les données lues par l'analyseur en blocs de données à analyser.



Il ne reste plus alors qu'à interpréter champ par champ, octet par octet ou bit par bit, le résultat.

1) En-tête MAC

Champ	Valeur hexa.	Commentaires
Adresse destination	00 A0 24 BD 75 BD	00 A0 24 Identification du fournisseur 3COM BD 75 BD N° séquentiel de fabrication de la carte
Adresse source	08 00 02 05 2D FE	08 00 02 Identification du fournisseur (ici 3 COM-Bridge)
Type de protocole	08 00	IP du DoD

2) En-tête IP

Champ	Valeur Hex.	Commentaires
Identification Version	4 -	Sur 4 bits, IP version 4
Longueur en-tête	- 5	IHL (*Internet Head Length*), sur 4 bits, en multiple de 4 octets la valeur normale est 5 soit 20 octets (pas d'option).
Type de service	00	Champ de bits Priorité (routine) - - - - - 0 0 0 Délai acheminement (Normal) - - - - 0 - - - Débit (Normal) - - - 0 - - - - Fiabilité (Normale) - - 0 - - - - - Réservés 0 0 - - - - - -
Longueur totale	00 60	Exprime la longueur totale du datagramme (données utiles de la couche MAC). Ici, la valeur 60 soit 96 octets est supérieure à 48, il n'y a donc pas eu d'opération de bourrage.
Identification	3C EF	Identifie tous les fragments d'un même datagramme.
Drapeau	00	Sur les trois derniers bits bit 7, non utilisé bit 6, DF (*Don't Fragment*), à 0 : fragmentation possible bit 5, MF (*More Fragment*), à 1indique qu'un fragment suit. Les autres bits appartiennent au champ suivant.
Offset	00	Sur 13 bits, indique la position du fragment depuis le début.
Durée de vie	1C	Time to Live, durée de vie du fragment, initialement exprimé en seconde, représente aujourd'hui le nombre de bonds restants.
Protocole supérieur	06	Identifie TCP
Total de contrôle	A4 FE	
@ IP Source	80 00 64 01	@IP = 128.0.100.1, Adresse de classe B.
@ IP Destination	DO 80 08 29	@IP = 208.128.8.41, Adresse de classe C. En principe, les machines sur un même réseau appartiennent à un même espace d'adressage. Ce n'est pas le cas ici. On peut donc penser que la machine source n'est pas sur le même réseau physique que la station destinataire du message.

3) En-tête TCP

FF FB 01 FF FD 01 0D 0A 0D 0A .r.....
0040: 55 4E 49 58 28 72 29 20 53 79 73 74 65 6D 20 56 UNIX(r) System V
0050: 20 52 65 6C 65 61 73 65 20 34 2E 30 20 28 63 65 Release 4.0 (ce
0060: 76 73 61 30 30 29 0D 0A 0D 00 0D 0A 0D 00 sa00).....

Le champ de données, reproduit ici, est partiellement décodé par l'analyseur (caractères interprétables). Cependant, l'analyse des premiers caractères du champ présente un intérêt certain : 'FF FB 01' et 'FF FD 01' sont des commandes TELNET (négociation d'options).

Toutes les commandes Telnet débutent par 'FF' (IAC, Interpret As Command, interpréter l'octet suivant comme une commande), si ce caractère apparaît dans le champ données il est doublé (caractère de transparence).

Le caractère suivant identifie la commande, il est éventuellement suivi d'un caractère qui précise une ommande optionnelle. Les tableaux des figures 20.32 et 20.33 fournissent la liste des principales commandes et des options Telnet.

Commande	Valeur dec.	Valeur Hex.	Signification
IAC	255	FF	Interpréter le caractère suivant comme une commande
DON'T *xx*	254	FE	Refus d'une option, le caractère suivant '*xx*' identifie l'option refusée
DO *xx*	253	FD	Acceptation de l'option '*xx*' (Start Use)
WON'T *xx*	252	FC	Acquittement négatif de l'option '*xx*'
WILL *xx*	251	FB	Acquittement positif de l'option '*xx*' (Will Use)
GA	249	F9	Continuer (Go Ahead)
EL	248	F8	Effacer une ligne (Erase Line)
EC	247	F7	Effacer un caractère (Erase Character)
AO	245	F5	Arrêter l'édition (Abort Ouput)
IP	244	F4	Interrompre le processus (Interrupt Process)
BRK	243	F3	Break
NOP	241	F1	Opération nulle (Non OPeration)
EOR	239	EF	Fin d'enregistrement (End of Record)

Figure 20.32 – Exemples de commandes Telnet.

Figure 20.33 – Exemples d'options Telnet.

Dialogue Telnet, paramétrage de l'écho :
'FF FB 01' IAC WILL ECHO, Will Use Echo Data
'FF FD 01' IAC DO ECHO, Start Use Echo Data

5) Champ FCS de la trame MAC
Valeur du FCS : 9F 59 6E FC

B – Décodage Trame MAC 2 (figure 20.34)

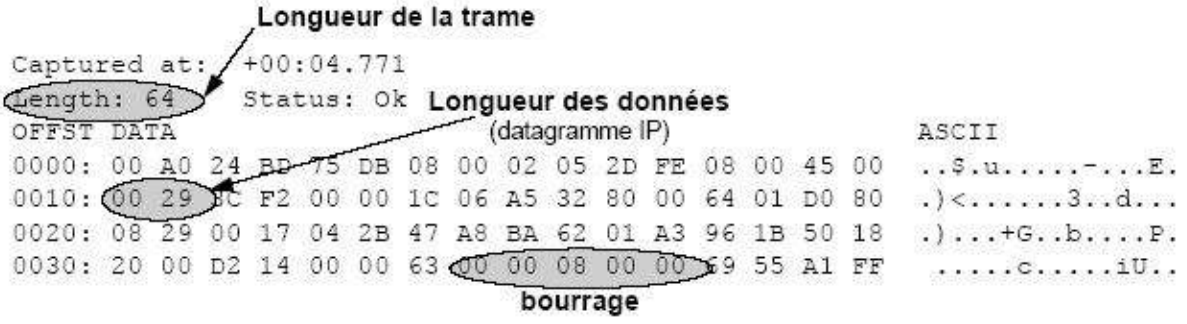


Figure 20.34 – Trame MAC numéro 2.
L'analyseur précise que la longueur de la trame MAC est de 64 octets (figure 20.34), c'est-à-dire la longueur minimale d'une trame MAC Ethernet.
Lorsque les données à transmettre ont une longueur inférieure à 64 octets, la couche MAC procède à un bourrage pour ramener la longueur du champ données MAC à 46 octets (64 octets en-tête MAC et FCS compris).
Si on examine le champ longueur du datagramme IP (figure 12.29) on constate qu'effectivement la longueur du datagramme est de 0x29 (41 octets), il y a donc 5 octets de bourrage, ces 5 octets sont quelconques, c'est le contenu du buffer

Annexes - Analyse TCP/IP

Structure d'une trame Ethernet

802.3 Ethernet packet and frame structure

Préambule	SFD	MAC dst	MAC src	Ethertype	Message	CRC
7	1	6	6	2	46 -- 1500	4

Preamble and start frame delimiter , Frame check sequence (32‑bit CRC); Start of frame delimiter

Structure d'un paquet IP

En-tête IPv4

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version d'IP				Lg en-tête				Type de service								Longueur totale															
Identification																Indicateur			Fragment offset											
Durée de vie								Protocole								Somme de contrôle de l'en-tête															
Adresse source																															
Adresse destination																															
Données : Option(s) + remplissage																															

Structure d'un datagramme UDP

Le paquet UDP est encapsulé dans un paquet IP. Il comporte un en-tête suivi des données à transporter.

En-tête IP	En-tête UDP	Données

L'en-tête d'un datagramme UDP est plus simple que celui de TCP :

Port Source (16 bits)	Longueur (16 bits)
Port Destination (16 bits)	Somme de contrôle (16 bits)
Données (longueur variable)	

Structure d'un datagramme TCP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Port Source																Port destination															
Numéro d'ordre																															
Numéro d'accusé de réception																															
Décalagedonnées				réservée						URG		ACK		PSH		RST		SYN		FIN	Fenêtre										
Somme de contrôle																Pointeur d'urgence															
Options																															
Remplissage																															
Données																															

Signification des différents champs :

- ✓ **Port Source** (16 bits): Port relatif à l'application en cours sur la machine source
- ✓ **Port Destination** (16 bits): Port relatif à l'application en cours sur la machine de destination
- ✓ **Numéro d'ordre** (32 bits): Lorsque le drapeau SYN est à 0, le numéro d'ordre est celui du premier mot du segment en cours. Lorsque SYN est à 1, le numéro d'ordre est égal au numéro d'ordre initial utilisé pour synchroniser les numéros de séquence (ISN)
- ✓ **Numéro d'accusé de réception** (32 bits): Le numéro d'accusé de réception également appelé numéro d'acquittement correspond au numéro (d'ordre) du prochain segment attendu, et non le numéro du dernier segment reçu.
- ✓ **Décalage des données** (4 bits): il permet de repérer le début des données dans le paquet. Le décalage est ici essentiel car le champ d'options est de taille variable
- ✓ **Réservé** (6 bits): Champ inutilisé actuellement mais prévu pour l'avenir
- ✓ **Drapeaux (flags)** (6x1 bit): Les drapeaux représentent des informations supplémentaires :
  - o **URG**: si ce drapeau est à 1 le paquet doit être traité de façon urgente.
  - o **ACK**: si ce drapeau est à 1 le paquet est un accusé de réception.
  - o **PSH** (PUSH): si ce drapeau est à 1, le paquet fonctionne suivant la méthode PUSH.
  - o **RST**: si ce drapeau est à 1, la connexion est réinitialisée.
  - o **SYN**: Le Flag TCP SYN indique une demande d'établissement de connexion.
  - o **FIN**: si ce drapeau est à 1 la connexion s'interrompt.
- ✓ **Fenêtre** (16 bits): Champ permettant de connaître le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception
- ✓ **Somme de contrôle** (Checksum ou CRC): La somme de contrôle est réalisée en faisant la somme des champs de données de l'en-tête, afin de pouvoir vérifier l'intégrité de l'en-tête
- ✓ **Pointeur d'urgence** (16 bits): Indique le numéro d'ordre à partir duquel l'information devient urgente
- ✓ **Options** (Taille variable): Des options diverses
- ✓ **Remplissage**: On remplit l'espace restant après les options avec des zéros pour avoir une longueur multiple de 32 bits