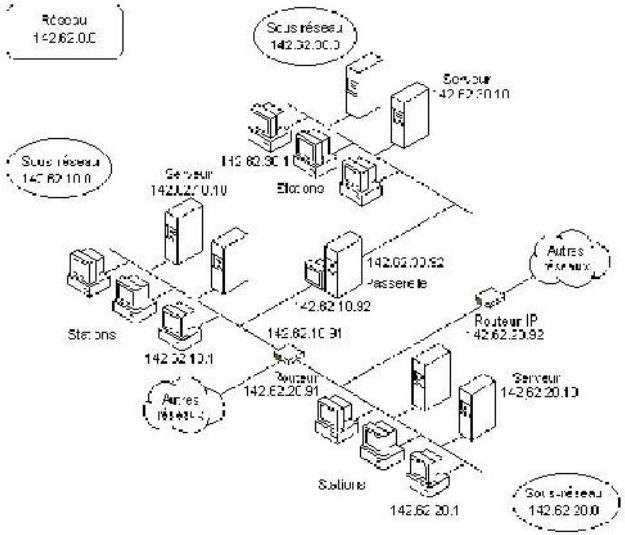
TD4 – Compléments

Exercice 1 : Table de Routage

A partir du schéma du réseau 142.62.0.0 suivant, dont le numéro de sous réseau est 255.255.255.0. Répondez, le plus précisément possible, aux questions ci-après.



1. Pourquoi la passerelle placée au milieu du schéma possède-t-elle deux adresses IP ?
2. Donnez une table de routage possible pour le routeur 142.62.10.91
3. Décrivez toutes les étapes du routage effectuées dans le réseau quand le serveur 142.62.20.10 adresse un paquet à la station 142.62.30.1. On suppose que serveurs comme stations ne connaissent que leur numéro IP, le masque de sous réseau et le numéro IP d'une passerelle par défaut.

Question 1 : Une adresse IP doit être affectée à chaque carte réseau. Ceci permet à la passerelle d'être connectée physiquement à deux réseaux distincts

Question 2 :

Réseau	Masque	Passerelle
142.62.10.0	255.255.255.0	142.62.10.91
142.62.20.0	255.255.255.0	142.62.20.91
142.62.30.0	255.255.255.0	142.62.10.92

Question 3 :

Le serveur 142.62.20.10 applique le masque de sous réseau à son adresse et à celle du destinataire, il trouve une différence, donc le destinataire n'est pas sur le même réseau.

Le serveur 142.62.20.10 envoie le paquet à sa passerelle par défaut : 142.62.20.91

La passerelle (le routeur) 142.62.20.91 applique le masque de sous réseau et trouve le numéro de sous réseau du destinataire : 142.62.30.0.

La passerelle trouve dans sa table de routage la correspondance 142.62.10.92 pour ce sous-réseau et lui envoie le paquet.

La passerelle 142.62.10.92 adresse finalement le paquet à la station 142.62.30.1 par le biais de son interface 142.62.30.92.

Exercice 2 : Table de Routage

6-3. 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 :

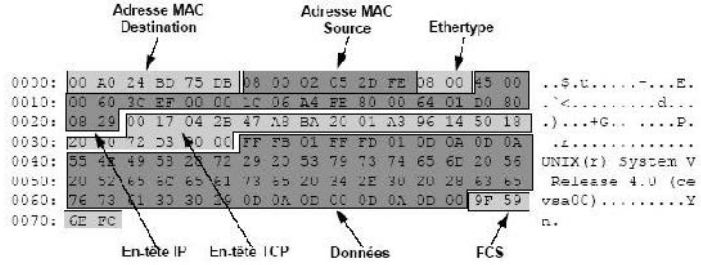
La trace proposée est une reproduction d'une trace obtenue avec un analyseur de protocole Ethernet. L'analyseur extrait le préambule, les fanions et ne présente que les données utiles. Le contenu de la trame en hexadécimal est interprété (codage ASCII), ce qui facilite le travail d'analyse.

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).

b) 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 sonds restants.
Protocole supérieur	06	Identifie TCP
Total de contrôle	A4 FE	
@ IP Source	80 00 34 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 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.

Exemples de commandes 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)

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

Exercice 3 : Table de Routage

Un réseau Ethernet utilisant le protocole TCP/IP est composé de différents segments. Les postes sont des clients Windows et des serveurs 2008.
Vous disposez d'une liste non exhaustive d'adresses IP utilisées dans ce réseau :

- 200.100.40.11 ; 200.100.40.1 ; 200.100.40.2 ; 200.100.50.11 ; 200.100.50.1 ; 200.100.60.11 ; 200.100.60.1

On vous fournit les deux tables de routage suivantes éditées à l'aide de la commande **netstat -r** sur 2 postes Windows du réseau appelés R1 et R2 :

Poste R1	Adresse réseau	Masque réseau	Adresse passerelle	Interface
	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
	200.100.40.0	255.255.255.0	200.100.40.1	200.100.40.1
	200.100.40.1	255.255.255.255	127.0.0.1	127.0.0.1
	200.100.40.255	255.255.255.255	200.100.40.1	200.100.40.1
	200.100.50.0	255.255.255.0	200.100.50.1	200.100.50.1
	200.100.50.1	255.255.255.255	127.0.0.1	127.0.0.1
	200.100.50.255	255.255.255.255	200.100.50.1	200.100.50.1
	200.100.60.0	255.255.255.0	200.100.40.2	200.100.40.1
	224.0.0.0	224.0.0.0	200.100.40.1	200.100.40.1
	224.0.0.0	224.0.0.0	200.100.50.1	200.100.50.1
	255.255.255.255	255.255.255.255	200.100.50.1	200.100.50.1

Poste R2	*Adresse réseau*	*Masque réseau*	*Adresse passerelle*	*Interface*
	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
	200.100.40.0	255.255.255.0	200.100.40.2	200.100.40.2
	200.100.40.2	255.255.255.255	127.0.0.1	127.0.0.1
	200.100.40.255	255.255.255.255	200.100.40.2	200.100.40.2
	200.100.60.0	255.255.255.0	200.100.60.1	200.100.60.1
	200.100.60.1	255.255.255.255	127.0.0.1	127.0.0.1
	200.100.60.255	255.255.255.255	200.100.60.1	200.100.60.1
	224.0.0.0	224.0.0.0	200.100.40.2	200.100.40.2
	224.0.0.0	224.0.0.0	200.100.60.1	200.100.60.1
	255.255.255.255	255.255.255.255	200.100.60.1	200.100.60.1

1. Interprétez les 5 premières lignes de la table de routage R2 , puis interprétez la 8eme ligne de la table de routage R1.
2. Quel rôle peuvent jouer les postes R1 et R2 sur le réseau ? Aidez-vous du contenu de la colonne Interface des tables de routage pour argumenter votre réponse. Décrivez une configuration matérielle et logicielle qui permette à ces postes d'assumer ce rôle
3. A l'aide de ces 2 tables de routage et de la liste des postes, faites le schéma logique du réseau correspondant
4. Écrivez la table de routage du poste 200.100.50.11, sachant que sur Windows la route par défaut s'exprime par 0.0.0.0
5. A partir du poste 200.100.50.11
   vous exécutez la commande suivante : **ping 200.100.60.11**
   La réponse à cette commande est : **request timed out**
   Pourquoi ? Que faut-il faire pour remédier à cela ?

6. Quelle commande IP permet d'établir la liste des routeurs qui sont sollicités lors de l'envoi d'un message ?

Correction

Question 1 :

Une ligne de table de routage se lit ainsi :
Pour joindre "telle adresse IP" dont la partie réseau est "composée ainsi", je dois passer par "tel routeur" et pour joindre ce routeur je dois utiliser "telle interface réseau".

Pour comprendre la première ligne il faut connaître l'adresse de réseau de bouclage 127.0.0.0. L'adresse 127.0.0.1 est l'adresse de loopback (ou de Localhost), elle signifie "mon adresse IP", c'est à dire l'adresse qui désigne le poste ou se trouve cette table.

Les masques de sous-réseau sont tous 255.255.225.0, la partie adresse réseau est donc représentée par les 3 premiers éléments de la notation décimale pointée. Nous pouvons en déduire que nous sommes soit en présence d'un réseau de

classe C, soit d'un sous réseau de classe A ou B. Or le premier octet de chaque adresse vaut 200 (soit **110**01000 en binaire). Nous sommes donc ici typiquement en classe C.

La deuxième ligne commence par l'adresse IP 200.100.40.0. La dernière partie de l'adresse IP à zéro signifie qu'on adresse le réseau logique 200.100.40.0 (tous les bits de la partie hôte sont à zéro, c'est donc une adresse de réseau ou adresse "this"). Donc pour atteindre ce réseau je dois passer par la passerelle 200.100.40.2 et utiliser pour cela mon interface réseau (ma carte réseau) qui a l'adresse IP 200.10.40.2, c'est à dire qu'en réalité je n'utilise pas de routeur puisque je reste à l'intérieur de mon réseau.

La troisième ligne se comprend facilement : pour m'atteindre moi-même, je passe par moi-même (route identique à l'adresse de loopback).

La quatrième ligne commence par une adresse de diffusion dirigée(directed broadcast). Pour adresser tous les postes du réseau 200.100.40.0, réseau dont je fais partie, j'utilise ma propre interface, (ici l'adresse 255.255.255.255 permet de faire la même chose dans la stricte cadre de mon réseau, alors qu'une adresse dirigée me permet un broadcast sur un autre réseau).

La cinquième ligne me permet d'atteindre le réseau 200.100.60.0 (autre réseau), pour cela je passe par le routeur 200.100.60.1 et pour l'atteindre j'utilise l'interface 200.100.60.1, ce qui sous entend que je l'atteins directement. Mon poste dispose d'une deuxième interface réseau, et ma table de routage me permet de m'orienter sur ces 2 interfaces.

La huitième ligne de la table du poste R1 permet d'atteindre le réseau 200.100.60.0 en passant par le routeur 200.100.40.2 et en utilisant l'interface 200.100.40.1. Ici nous utilisons un deuxième routeur pour accéder à ce réseau, nous ne l'atteignons pas directement, nous accédons d'abord au routeur 200.100.40.2 en utilisant notre interface 200.100.40.1 et ce routeur se débrouillera (il inspectera sa table) pour atteindre le réseau cible.

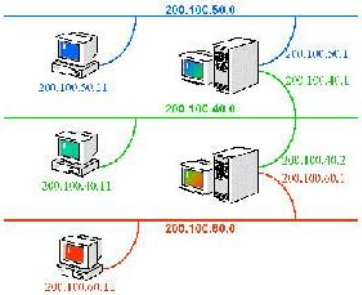
Remarque : l'adresse commençant par 224 est une adresse réservée utilisée par l'adressage multipoint.

Question 2 :

Quand on lit la colonne interface de ces deux tables, on s'aperçoit que les postes 1 et 2 disposent chacun de 2 cartes réseaux, ils peuvent donc jouer le rôle de routeur. Pour cela, ils doivent disposer du module IP : Ip forwarding. Ce sont des postes NT4. Dans la configuration réseau on a activé la fonction routage.

Chaque carte réseau sera connectée à un segment Ethernet, et chacune disposera de sa propre adresse IP.
Ces postes vont interconnecter les trois réseaux logiques :
200.100.40.0, 200.100.60.0 et 200.100.50.0

Question 3 :



Question 4 :

Ce poste ne joue pas le rôle de routeur, mais il doit connaître le poste routeur pour lui adresser les paquets non destinés au réseau (adresse de la passerelle dans la configuration IP)Avec TCP IP, chaque poste est actif et dispose d'une table de

routage même s'il n'est pas routeur. Le poste 200.100.50.11 ne déroge pas à la règle, la lecture de sa première ligne nous permet d'identifier son routeur. La colonne interface nous indique qu'il n'a qu'une seule interface réseau.

Poste 200.100.50.11

Adresse réseau	Masque réseau	Adresse passerelle	Interface
0.0.0.0	0.0.0.0	200.100.50.1	200.100.50.11
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
200.100.50.0	255.255.255.0	200.100.50.11	200.100.50.11
200.100.50.11	255.255.255.255	127.0.0.1	127.0.0.1
20.100.50.255	255.255.255.255	200.100.50.11	200.100.50.11
224.0.0.0	224.0.0.0	200.100.50.11	200.100.50.11
255.255.255.255	255.255.255.255	200.100.50.11	200.100.50.11

Question 5 :

Le ping au niveau interne est en fait une demande d'écho qui permet de tester entre autre un lien bidirectionnel (protocole ICMP).

Notre ping passe à travers les deux routeurs, ceux-ci doivent avoir leur table de routage prévue pour cela. R1 sait qu'il doit passer par R2 pour atteindre le réseau 200.100.60.0 mais la route de retour ne fonctionne pas, R2 ne sait pas qu'il doit passer par R1 pour atteindre le réseau 200.100.50.0 ; sa table de routage ne le lui indique pas.

Pour que notre ping fonctionne, il faut mettre à jour cette table ainsi :

(syntaxe Windows) **Route add 200.100.50.0 mask 255.255.255.0 200.100.40.1**

Cette commande indique à R2 que pour atteindre le réseau 200.100.50.0 il faut passer par la passerelle 200.100.40.1 (R1) et donc envoyer le paquet sur l'interface 200.100.40.2 (cette interface sera déduite automatiquement de la table de routage).

Question 6 :

Pour obtenir la liste des routeurs sollicités lors de l'envoi d'un message sur NT, on utilise la commande tracert qui à l'aide du protocole ICMP permet d'identifier les différents routeurs traversés. **tracert 200.100.60.11**

Remarque : Les commandes IP sont légèrement différentes entre UNIX et Windows, ayant visiblement voulu conserver des commandes sur 8 caractères.