

Partie 2 : Analyse d'échange de trames

Utiliser l'annexe 2 pour cette partie

Dans l'extrait d'enregistrement donné dans l'annexe 2, les trames N° 3 et 4 (1^{ère} et 2^{ème} de l'extrait) indiquent que le protocole ARP est utilisé.

- 2.1 Indiquer le rôle général du protocole ARP.**
- 2.2 Indiquer ce qu'il a permis d'obtenir comme informations dans le cas précis des trames N° 3 et 4 (1^{ère} et 2^{ème} de l'extrait), puis compléter le document à rendre avec la copie de l'annexe 4.**

Dans l'extrait d'enregistrement donné dans l'annexe 2, les trames N° 5 et 6 (3^{ème} et 4^{ème} de l'extrait) indiquent que le protocole DNS est utilisé.

- 2.3 Indiquer le rôle général d'un serveur DNS.**
- 2.4 Dans le cas de l'enregistrement quelle est l'adresse IP du serveur DNS qui est sollicité ?**
- 2.5 Indiquer ce qu'il a permis d'obtenir comme informations dans le cas précis des trames N° 5 et 6 (3^{ème} et 4^{ème} de l'extrait) puis compléter le document à rendre avec la copie de l'annexe 4.**

Dans l'extrait d'enregistrement donné dans l'annexe 2, les trames N° 7 et 8 (5^{ème} et 6^{ème} de l'extrait) indiquent qu'un des composants du réseau a l'adresse IP 192.168.0.1. En vous aidant de la configuration réseau de la station 192.168.0.5 et de la position de cet élément dans le réseau

- 2.6 Indiquer quelles fonctions (3 fonctions) remplit ce composant du réseau.**
- 2.7 Indiquer le rôle de chacune de ces trois fonctions.**

Dans l'extrait d'enregistrement donné dans l'annexe 2, les trames N° 9, 10 et 11 (7^{ème}, 8^{ème} et 9^{ème} de l'extrait) indiquent que le protocole TCP est utilisé

- 2.8 Quel est le rôle de ce protocole ?**
- 2.9 À quelle phase de la session correspondent ces 3 trames ? Puis compléter le document à rendre avec la copie de l'annexe 4.**

Les messages http des trames N° 14 et 15 sont encapsulés dans des segments TCP. Chacun des 2 segments a une longueur de 1420 octets.

- 2.10 Déterminer la valeur du compteur indiquant le numéro de séquence TCP (seq) de la trame N° 15**
- 2.11 Finir de compléter le document à rendre avec la copie de l'annexe 4 pour les trames 12,13,14,15.**

ANNEXE 2

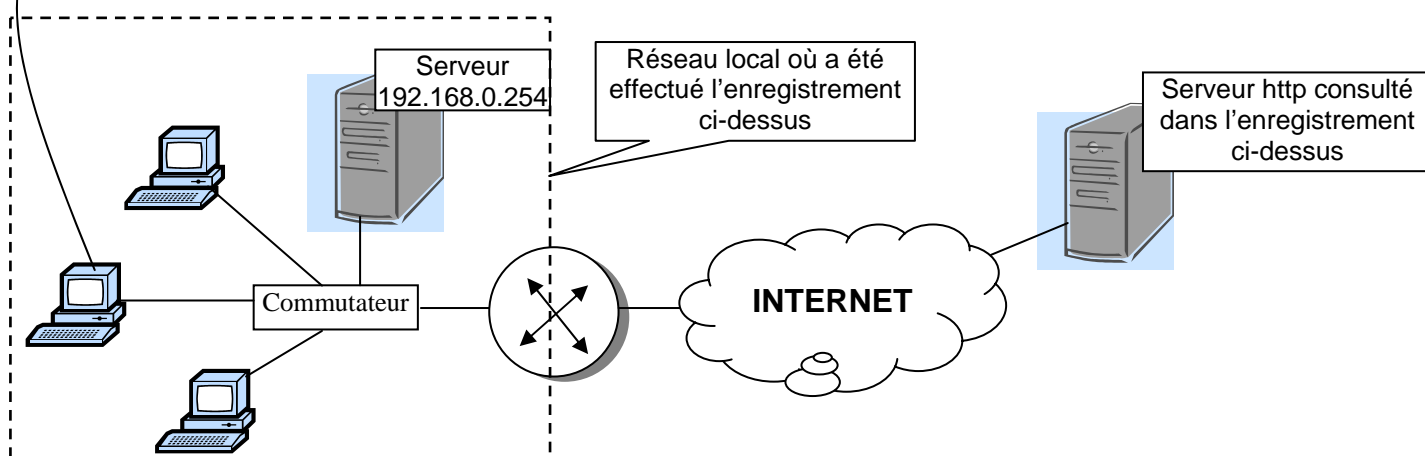
Extrait d'un enregistrement d'échanges de trames réalisé sur le réseau local suivant

No.	MAC Src	MAC Dest	IP Source	IP Dest	Protocol	Info
3	00:0b:db:84:cb:1d	ff:ff:ff:ff:ff:ff	00:0b:db:84:cb:1d	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.0.254? Tell 192.168.0.5
4	00:48:54:66:8c:d4	00:0b:db:84:cb:1d	00:48:54:66:8c:d4	00:0b:db:84:cb:1d	ARP	192.168.0.254 is at 00:48:54:66:8c:d4
5	00:0b:db:84:cb:1d	00:48:54:66:8c:d4	192.168.0.5	192.168.0.254	DNS	Standard query A www.mrim.net
6	00:48:54:66:8c:d4	00:0b:db:84:cb:1d	192.168.0.254	192.168.0.5	DNS	Standard query response A 80.65.224.232
7	00:0b:db:84:cb:1d	ff:ff:ff:ff:ff:ff	00:0b:db:84:cb:1d	ff:ff:ff:ff:ff:ff	ARP	who has 192.168.0.1? Tell 192.168.0.5
8	00:09:5b:2b:df:4e	00:0b:db:84:cb:1d	00:09:5b:2b:df:4e	00:0b:db:84:cb:1d	ARP	192.168.0.1 is at 00:09:5b:2b:df:4e
9	00:0b:db:84:cb:1d	00:09:5b:2b:df:4e	192.168.0.5	80.65.224.232	TCP	1363 > 80 [SYN] Seq=2138734067 Ack=0 win=
10	00:09:5b:2b:df:4e	00:0b:db:84:cb:1d	80.65.224.232	192.168.0.5	TCP	80 > 1363 [SYN, ACK] Seq=3062160243 Ack=2
11	00:0b:db:84:cb:1d	00:09:5b:2b:df:4e	192.168.0.5	80.65.224.232	TCP	1363 > 80 [ACK] Seq=2138734068 Ack=306216
12	00:0b:db:84:cb:1d	00:09:5b:2b:df:4e	192.168.0.5	80.65.224.232	HTTP	GET / HTTP/1.1
13	00:09:5b:2b:df:4e	00:0b:db:84:cb:1d	80.65.224.232	192.168.0.5	TCP	80 > 1363 [ACK] Seq=3062160244 Ack=213873
14	00:09:5b:2b:df:4e	00:0b:db:84:cb:1d	80.65.224.232	192.168.0.5	HTTP	HTTP/1.1 200 OK
15	00:09:5b:2b:df:4e	00:0b:db:84:cb:1d	80.65.224.232	192.168.0.5	HTTP	Continuation

Détails de connexion réseau

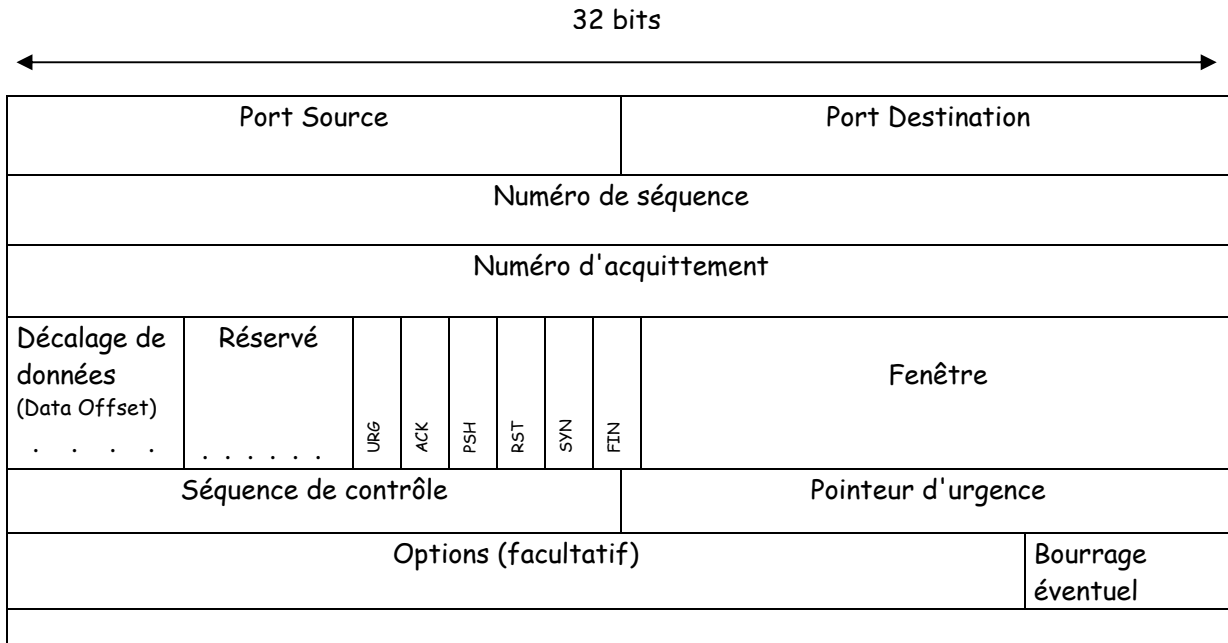
Détails de connexion réseau :

Propriété	Valeur
Adresse physique	00-0B-DB-84-CB-1D
Adresse IP	192.168.0.5
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	192.168.0.1
Serveur DHCP	192.168.0.1
Bail obtenu	01/02/2004 08:03:37
Bail expirant	04/02/2004 08:03:37
Serveurs DNS	192.168.0.254
	193.252.19.3
Serveur WINS	

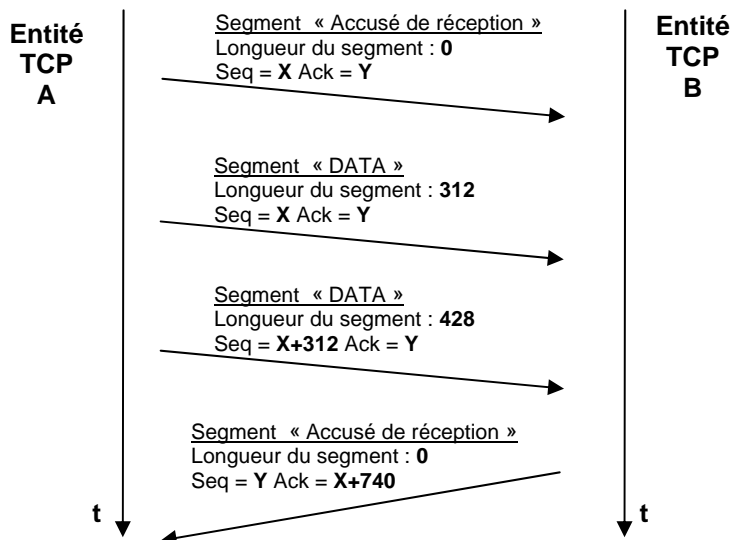


ANNEXE 3

Structure de l'en-tête TCP



Pendant la phase d'établissement de la connexion, les numéros de séquence initiaux sont échangés par les deux interlocuteurs. Ces numéros de séquence sont utilisés pour décompter les données dans le flux d'octets. On trouve toujours deux de ces nombres dans chaque segment TCP, qui sont le *numéro de séquence (seq)* et le *numéro d'acquittement (ack)*. Le *numéro de séquence* indique le numéro d'ordre du premier octet du segment envoyé, tandis que le *numéro d'acquittement* représente le numéro de séquence du destinataire.



ANNEXE 4

(Document à rendre avec la copie)

Après avoir indiqué dans le diagramme ci-dessous les adresses IP manquantes et les adresses MAC manquantes, représenter le diagramme fléché correspondant à l'échange de trames de l'enregistrement de l'annexe 2

