RES2	Les réseaux informatiques : Encapsulation

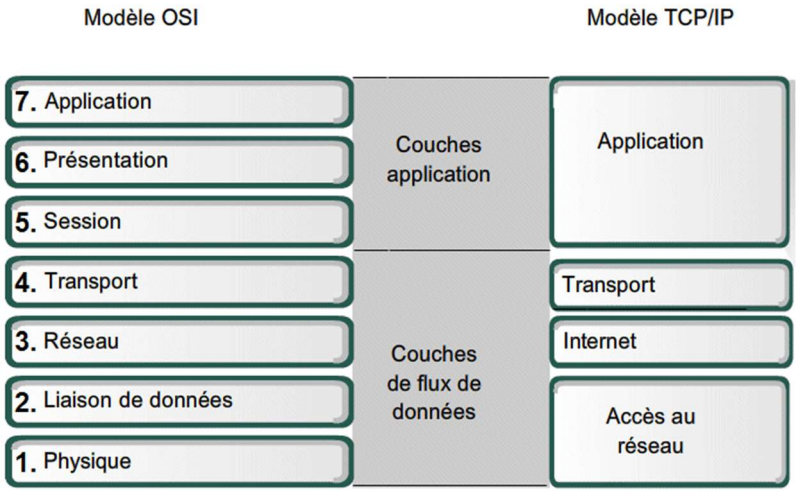
G.COLIN

Savoirs associés : Réseaux locaux industriels

Objectifs : ⇨ **Analyser une trame ETHERNET**
⇨ **Utilisation du logiciel WIRESHARK**

1) Présentation

Le modèle de référence OSI (Open Systems Interconnection) divise le processus de réseau en sept couches logiques, chacune comportant des fonctionnalités uniques et se voyant attribuer des services et des protocoles spécifiques.
Les protocoles TCP/IP ont été développés avant la définition du modèle OSI, et n'utilisent que 4 couches.

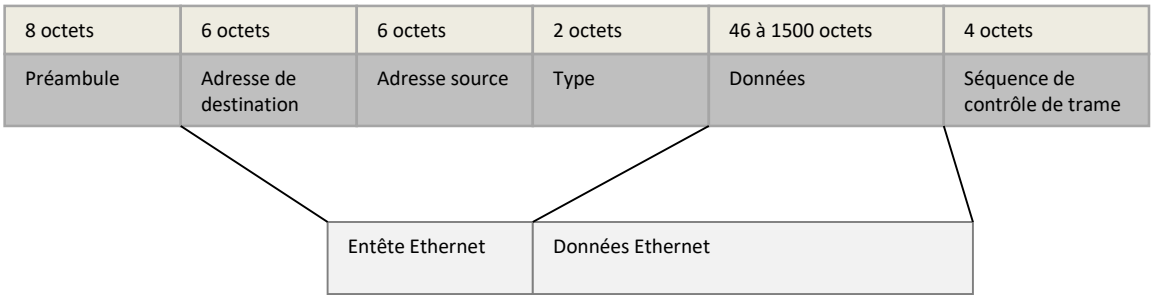


Correspondance entre Modèle OSI et Modèle TCP/IP

Sur les réseaux Ethernet et Internet, c'est le modèle TCP/IP qui est utilisé.

Application	HTTP, FTP, SMTP …
Transport	UDP, TCP ….
Internet	Adresse IP …
Accès réseau	MAC sur Ethernet …

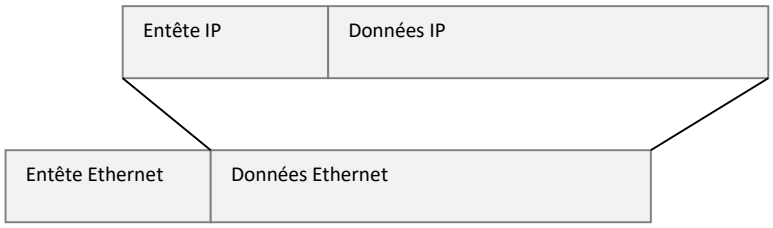
Trame ETHERNET (niveau accès réseau):



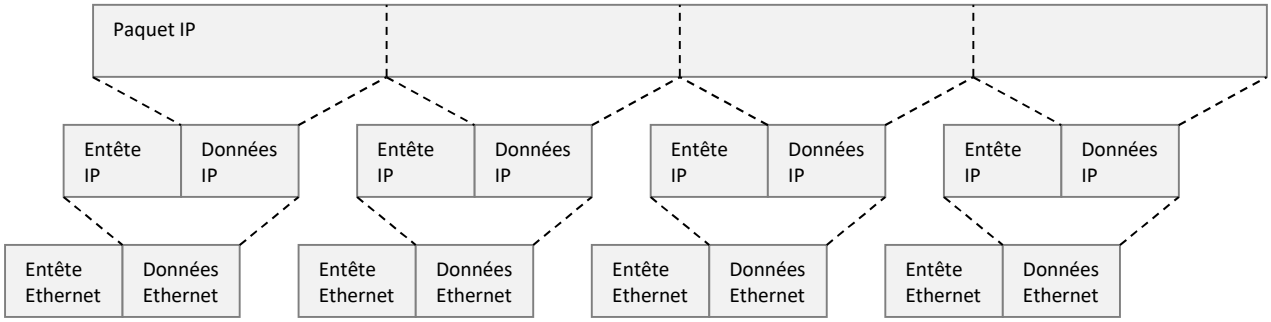
Le préambule sert à la synchronisation de l'horloge du récepteur.
La séquence de contrôle de trame permet de vérifier l'intégrité des données.
Les informations utiles pour l'utilisateur sont : l'adresse source, l'adresse de destination, le type et les données.

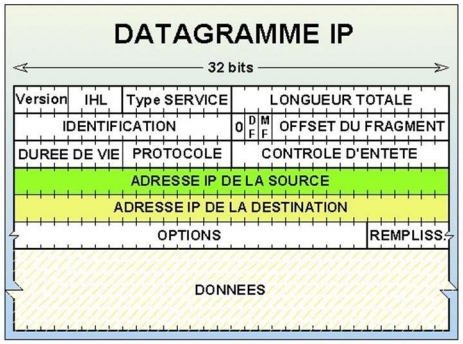
Paquets IP (niveau Internet) :

Sur un réseau Ethernet, les paquets IP sont encapsulés dans les données de la trame Ethernet.



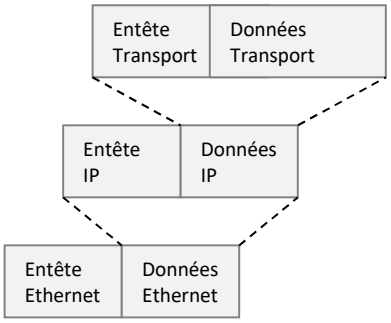
L'entête IP comporte, en autre, les adresses IP, le protocole, le numéro de segment, la version …
Un paquet IP peut contenir 64 K octets. Si la taille du paquet IP est supérieur à 1500 octets, le paquet est segmenté.





Couche transport

Les données de la couche transport sont encapsulées dans les données IP.



Les deux protocoles de la suite de protocoles TCP/IP les plus couramment employés sont le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol).
L'entête transport contient, notamment, des numéros de port qui identifient l'application.

Segment TCP

Bit (0)	Bit (15)	Bit (16)	Bit (31)
Port source (16)		Port de destination (16)	
Numéro d'ordre (32)			
Numéro de reçu (32)			
Longueur de l'en-tête (4) Réservé (6) Bits de code (6)		Fenêtre (16)	
Somme de contrôle (16)		Urgent (16)	
Options (0 ou 32 le cas échéant)			
DONNÉES DE LA COUCHE APPLICATION (Taille variable)			

20 octets

Datagramme UDP

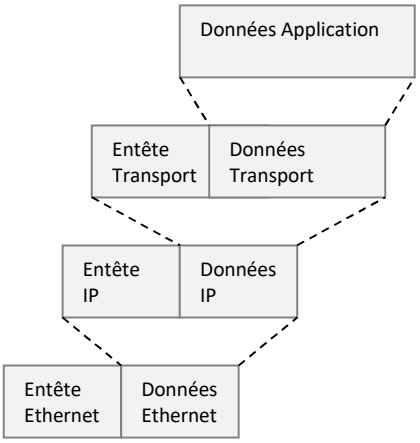
Bit (0)	Bit (15)	Bit (16)	Bit (31)
Port source (16)		Port de destination (16)	
Longueur (16)		Somme de contrôle (16)	
DONNÉES DE LA COUCHE APPLICATION (Taille variable)			

8 octets

Un segment TCP peut être découpé en plusieurs segments, et reconstitué à la réception.

Couche application

Les données de l'application sont encapsulées dans les données de la couche transport.



2) Adresse IP et adresse MAC

Demander au prof la configuration IP de la carte réseau à réaliser avant toute manipulation.

2.1 – Sous l'invite de commande (accessoires ⇨ invite de commande ou exécuter⇨cmd), tapez la commande « ipconfig/all » et relever sur le compte rendu (pour la carte relié au réseau du lycée):

- L'adresse physique (ou adresse MAC) en hexadécimale
- L'adresse IP
- L'adresse de la passerelle par défaut
- L'adresse du serveur DHCP
- L'adresse du serveur DNS

Un fichier appelé « Table ARP » mémorise la correspondance entre adresse physique et adresse IP. L'accès à cette table est réalisé par la commande arp –a.

2.2 – Sous l'invite de commande, tapez la commande « arp –a » et relever sur le compte rendu l'adresse physique de la passerelle du lycée (adresse IP relevée en 2.1).

NB : La passerelle (fonction routeur) fait la liaison entre le réseau internet et le réseau privé du lycée.

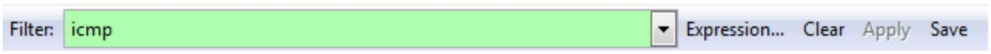
Utilisation de Wireshark – Acquisition d'une trame ping

Réclamer une démonstration au prof si les indications ci-dessous sont insuffisantes.

⇨ Lancer le logiciel Wireshark

⇨ Sélectionner l'interface utilisée : Connexion au réseau local

⇨ Appliquer le filtre utilisé : entrer « icmp » puis valider avec Apply



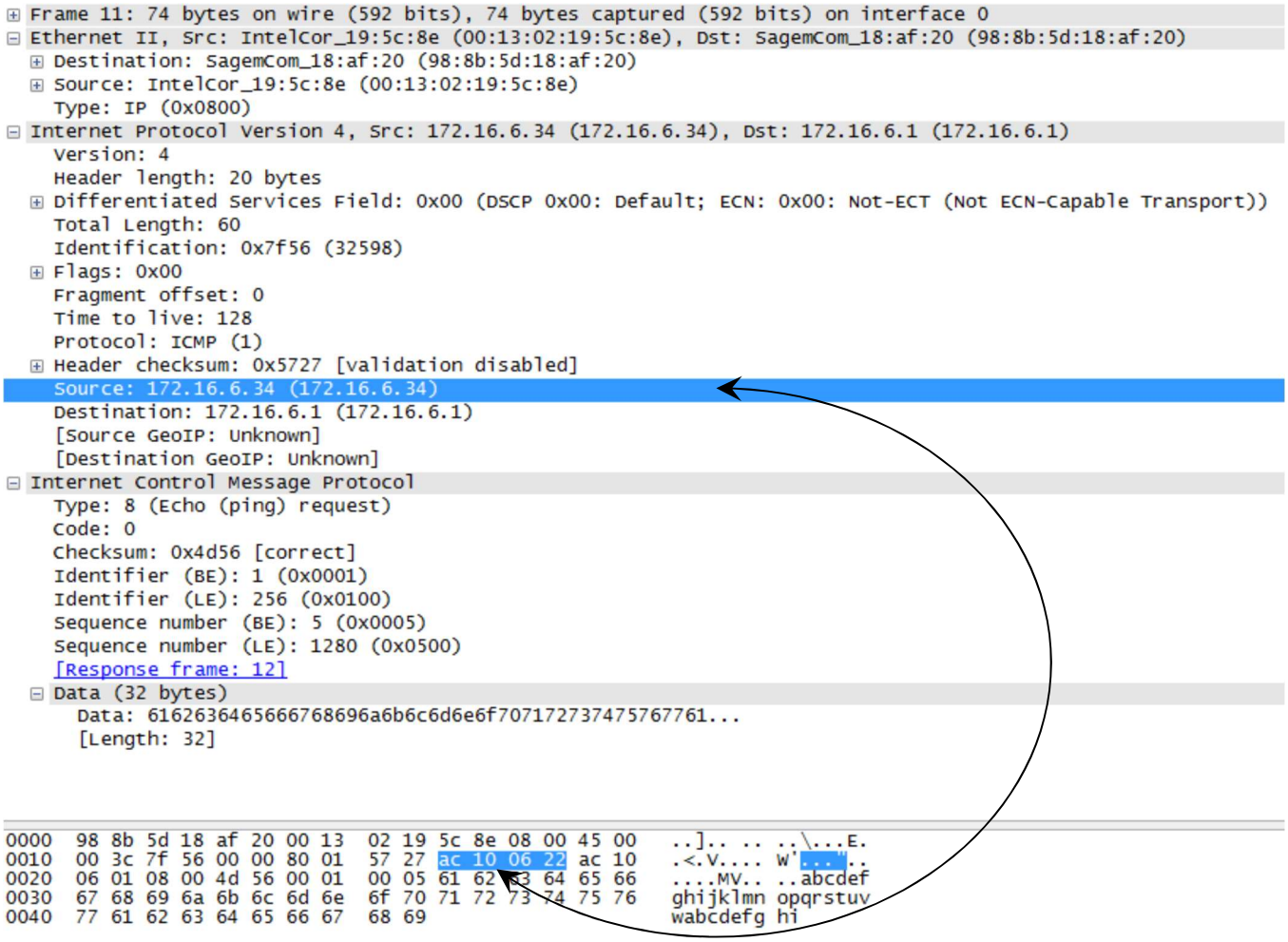
⇨ Lancer l'acquisition des trames en cliquant sur l'icône 

⇨ Sous l'invite de commande, faire un ping sur la passerelle (ping 172.16.0.253).

⇨ Sélectionner la première ligne d'acquisition comme ci-dessous :

No.	Time	Source	Destination	Protocol	Length	Info
11	17.563193000	172.16.6.34	172.16.6.1	ICMP	74	Echo (ping) request id=0x0001,
12	17.575478000	172.16.6.1	172.16.6.34	ICMP	74	Echo (ping) reply id=0x0001,
13	18.562335000	172.16.6.34	172.16.6.1	ICMP	74	Echo (ping) request id=0x0001,
14	18.590525000	172.16.6.1	172.16.6.34	ICMP	74	Echo (ping) reply id=0x0001,
15	19.576405000	172.16.6.34	172.16.6.1	ICMP	74	Echo (ping) request id=0x0001,
16	19.587299000	172.16.6.1	172.16.6.34	ICMP	74	Echo (ping) reply id=0x0001,
18	20.582028000	172.16.6.34	172.16.6.1	ICMP	74	Echo (ping) request id=0x0001,
19	20.589145000	172.16.6.1	172.16.6.34	ICMP	74	Echo (ping) reply id=0x0001,

⇨ Développer la trame pour faire apparaître les différents champs. En cliquant sur une donnée (exemple ici avec l'adresse IP source), on fait apparaître son emplacement dans la trame (notation hexa).



Remarque : le protocole ICMP n'utilise pas la couche transport. La trame ICMP est directement encapsulée dans les données IP.

2.3 – Sur le document réponse, pour une demande ICMP, reporter dans les 2 tableaux les adresses MAC, les adresses IP et le numéro du protocole ICMP.

2.4 – Encadrer (avec de la couleur) sur le premier tableau les entêtes Ethernet, IP et ICMP.

2.5 – Faire la même chose (questions 2.3 et 2.4) avec la réponse ICMP.

3) Numéro de port

Au lycée, pour accéder à internet, on passe par un proxy qui se trouve sur le serveur du lycée.
Un proxy est un programme servant d'intermédiaire pour accéder à un autre réseau, comme internet. Il filtre et surveille les échanges entre les 2 réseaux.

Généralement, un client http utilise le port 80. Avec l'utilisation du proxy, le client fait ses demandes au serveur du lycée sur le 3128.

⇨ Lancer une nouvelle acquisition avec Wireshark avec le filtre « http » (+ apply) (port 3128 ou 80 suivant le cas)

```
http && tcp.port==3128
```

⇨ Ouvrir Internet Explorer ou Firefox avec comme page d'accueil google.fr (demander au prof)

⇨ Arrêter l'acquisition des trames.

⇨ Sélectionner la première trame http (commande GET `GET http://www.google.fr/`) et développer les différentes couches.

3.1 – Sur le document réponse, reporter dans les 2 tableaux :

- les adresses MAC
- les adresses IP
- le numéro du protocole et la correspondance UDP ou TCP
- les numéros de port source et destination

3.2 – Encadrer (avec de la couleur) sur le premier tableau les entêtes Ethernet, IP et TCP.

3.3 – Par une recherche sur internet, indiquer les ports de destination utilisés par les applications FTP et SMTP.