Dans ce TP nous allons étudier le protocole ICMP (Internet Control Message Protocol). Associé à IP, il permet de transmettre des messages de contrôle ou d'erreurs (par exemple destinataire inaccessible, expiration de la durée de vie d'un paquet,…). Il est utilisé plus particulièrement par les programmes `ping` et `traceroute` dont vous allez analyser, avec l'outil `wireshark`, les messages générés.

À noter, il n'est pas nécessaire d'utiliser le cyber-range pour les exercices II, III, IV.

Récupérer les traces réseau pour ce TP sur Arche ou sur le lien ci-dessous :
- http://thibault.cholez.free.fr/teaching/RSI/TP_IP-ICMP_traces.zip

I. Table de routage IP et table ARP

Afficher la table de routage d'un des ordinateurs du réseau local avec la commande **netstat -nr** ou la commande **route**. Comment interprétez-vous les les deux routes ?

Générer des requêtes ARP pour les adresses IP du réseau local avec la commande : **arping adresse_IP -I interface** et observer les reqûetes et réponses ARP qui transitent avec wireshark.

Afficher maintenant la table avec la commande **sudo arp -v -n** et vérifier que les couples @IP/@MAC ont bien été mis en cache.

II. Messages ICMP générés par le programme `ping`

`ping` est un programme qui permet de vérifier qu'une machine est « vivante » ou non, c'est-à-dire qu'elle est accessible au niveau de la couche 3. La source envoie (ping) un paquet vers une adresse IP et si la destination est accessible, elle répond (pong) en renvoyant le paquet à son tour vers la machine source.

1) Mesurer la valeur du RTT avec la commande `ping` vers les machines suivantes:
   - votre passerelle par défaut (trouvable grâce à la commande `route`, il s'agit de la gateway pour la route par defaut 0.0.0.0)
   - le serveur web de l'école (www.telecomnancy.univ-lorraine.fr)
   - des serveurs web en France (ex : www.orange.fr, www.free.fr)
   - des serveurs web en Europe (ex : www.tu-darmstadt.de, etzh.ch)
   - des serveurs web aux USA (ex : www.berkeley.edu, www.mit.edu, www.univcan.ca)
   - des serveurs web en Asie (ex : www.nict.go.jp, postech.ac.kr)

- Faire en sorte que votre commande s'arrête automatiquement après l'envoi de 5 paquets ICMP (faire un man de `ping`).
- En déduire les classes de latence en fonction de la distance au serveur (campus, ville, pays, continent, monde).
- La latence du site www.mit.edu semble faible au regard de sa distance, comment pouvez-vous expliquer cela ? Indice : renseignez vous sur ce qu'est un Content Delivery Network comme Akamai).
- Pour info : la carte des câbles sous-marins : https://www.submarinecablemap.com

2) Copier dans votre répertoire le *icmp-wireshark-trace-1 et* l'ouvrir ensuite avec `wireshark`.

Analyse en-tête IP

Positionnez-vous sur le premier paquet et répondez aux questions suivantes :

- Quelle est l'adresse IP de la machine réalisant la commande `ping` ?
- Quelle est l'adresse IP de la machine destination ?
- Dans l'en-tête IP, quelle est la valeur du champ protocol ?
- Combien d'octets dans l'en-tête IP ? Comment est codée la longueur de l'en-tête IP dans le paquet IP ?
- Combien d'octets dans la partie payload du datagramme IP ? Expliquer comment est déterminé ce nombre d'octets ?

Analyse paquet ICMP

- Un paquet ICMP a-t-il un numéro de port ?
- Examiner le premier paquet *ICMP echo request* envoyé par la source :
  - Quels sont le type ICMP et le numéro de code ?
  - Quels sont les autres champs du paquet ICMP ?
  - Comment évolue le champ **Identifier** entre les différents *ICMP echo request ?* De même le champ **Sequence Number** ?
- Examiner le paquet *ICMP reply* correspondant à la requête.
  - Quels sont le type ICMP et le numeros de code ?
  - Quels sont les autres champs du paquet ICMP ? Comment est établi le lien avec la requête ?
- Combien de requêtes ont été envoyées pour la même commande `ping` ?
- Combien de commandes `ping` ont été effectuées ?

III. Messages ICMP générés par le programme Traceroute

Traceroute est un programme qui permet de détecter l'ensemble des passerelles entre une source et une destination. Le programme est implanté de manière différente sous Unix et Windows. Avec Unix, la source envoie une série de paquets UDP vers la destination en utilisant des numéros de ports improbables (très élevés). Avec Windows, la source envoie une série de paquets ICMP vers la destination. Dans les deux cas, le programme envoie le premier paquet avec un TTL=1, le second paquet avec un TTL =2,…
Le champ TTL dans un en-tête IP est décrémenté de 1 à chaque traversée de routeurs/passerelles. Quand le paquet arrive au niveau d'un routeur avec la valeur de 1, il n'est pas retransmis et un paquet ICMP est renvoyé. Cela permet d'éviter que des paquets tournent indéfiniment dans le réseau.

1) Faire un traceroute (commandes tracepath/traceroute sous Linux ou tracert sous windows) vers :
   - venus.telecomnancy.eu
   - www.google.com

     Combien mesurez-vous de routeurs intermédiaires pour chacune de ces deux destinations ?

2) Copier dans votre répertoire le fichier *icmp-wireshark-trace-2 et* l'ouvrir ensuite avec `wireshark`.
   - Trier les paquets selon le champ information en cliquant sur l'onglet *Info.* Sélectionner le premier message UDP envoyé.
     - Quelles est la valeur du champ TTL pour les 3 premiers messages, les 3 suivants et ainsi de suite.
     - Comment évolue le numéro de port ?

- Combien de messages UDP sont envoyés pour le traceroute ?
- En déduire le nombre de routeurs séparant la source de la destination.
- A quel site correspond l'adresse destination (cf question II. 1)) ?

- Trier les paquets selon le champ Numéro en cliquant sur l'onglet *No.* Sélectionner le premier message *ICMP TTLexceeded* envoyé à la source par le routeur le plus proche.
  - Quels sont le type ICMP et le numéro de code ?
  - Analyser les données contenues dans le paquet ICMP.
- Se positionner sur les 3 derniers messages ICMP.
  - Quels sont le type ICMP et le numéro de code ?
  - En déduire comment la source détermine la fin du traceroute.
  - Analyser les données contenues dans le paquet ICMP.

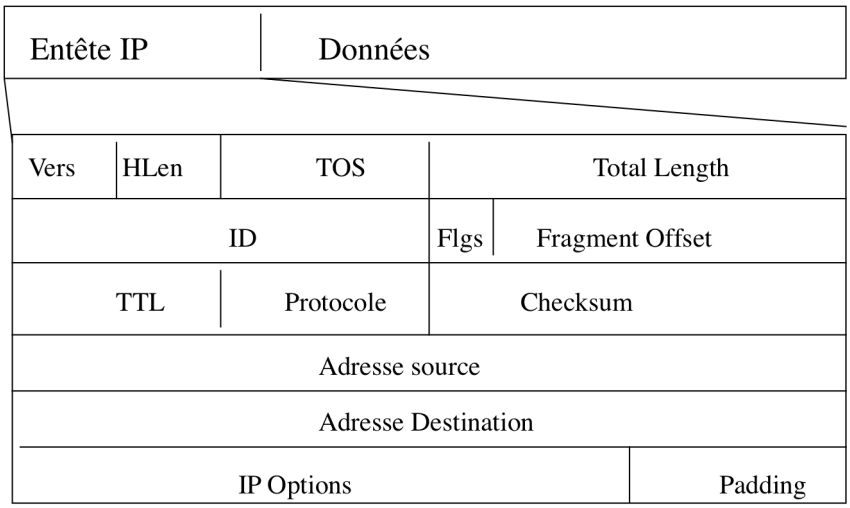
IV. Fragmentation IP

Copier dans votre répertoire le fichier *icmp-wireshark-trace-3 et* l'ouvrir ensuite avec `wireshark`. Positionnez-vous sur le paquet numéro 1.

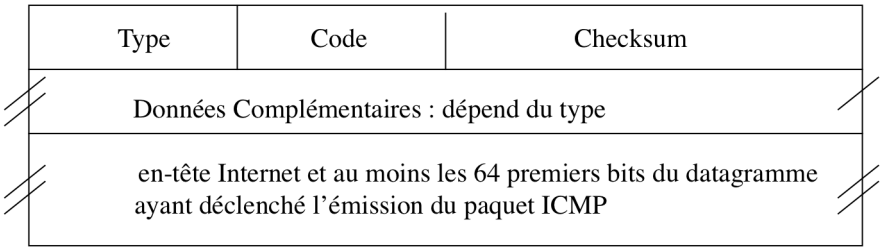
- Quelle information dans l'en-tête IP indique que le paquet a été fragmenté ?
- En combien de fragments a été découpé le message ?
- Quelle information indique qu'il s'agit du premier ou du dernier fragment ?
- Quelle est la taille du message ICMP (sans l'en-tête ICMP) ?
- Vérifier votre réponse en regardant les données incluses dans le paquet ICMP Reply.
- Quelle est à votre avis la taille du MTU ?
- A quoi correspondent les paquets n° 4 et 5 ?

ANNEXES

En-tête IP



En-tête ICMP


Type
Code
Checksum
Données Complémentaires : dépend du type
en-tête Internet et au moins les 64 premiers bits du datagramme ayant déclenché l'émission du paquet ICMP