TP 3 :

# Messages CIMP générés par le programme **Ping**

2)

## Analyse IP :

* IP :
  + Source : 152.81.15.95
  + Destination : 152.81.1.1

En-tête IP : 20 octets

Longueur de l’en-tête codée en 4 bits : à multiplier par 32 pour avoir la table réelle

Longueur du payload = longueur totale – longueur de l’entête

Valeur du champ protocole = 1 (ICMP)

## Analyse ICMP

* Aucun numéro de port car il s’agit d’un protocole de niveau réseau
* ICMP Echo :
  + Code désignant le type de message :
    - Echo : 8
    - Reply : 0
  + Autres champs :
    - Checksum (2 octets)
    - Numéro de séquence (2 octets)
    - ID (2 octets)
    - Timestamp (8 octets)
    - Données (48 octets)
  + Identifier : Reste inchangé Mais numéro de séquence incrémenté à chaque envoie de paquet IP
* ICMP reply
  + On a :
    - Type : 0
    - Numéro de séquence : 0
  + Autres champs :
    - Checksum (2 octets)
    - Numéro de séquence (2 octets)
    - ID (2 octets)
    - Timestamp (8 octets)
    - Données (48 octets)
* Il y a eu 10 requêtes ping (ping -c 10 ADRESSE\_IP)
* Il y a eu deux commandes ping

# Messages ICMP génères par le programme Traceroute

* UDP Envoyé
  + Le premier paquet est à un et les suivants sont incrémentés
  + Il y a 3 paquets UDP envoyé pour le traceroute
  + Il y a 9 équipements entre la source et la destination   
    Message avec TTL = 10
* Message ICMP TTLexceeded
  + On a :
    - Type ICMP : type 11, code 0
    - Destination unreable (Type 3)
    - Port unreable (code 3)
* 3 derniers messages ICMP
  + Paquet ICMP = en-tête du paquet en erreur (20 octets) + en-tête UDP du paquet en erreur (8 octets) + 24 premiers octets du paquet en erreur
  + La fin du traceroute à lieu qua

# Fragmentation IP

* Le champ : More Fragment : 1
* 2 Fragments + 1 (ICMP reconstitué) = 3 fragments
* 1er fragment,
  + Offset = 0
* Dernier fragment :
  + More fragment = 0
* Taille du message ICMP -> 1480 (-8) + 1480 + 48 = 3000
* MTU = 1480 + 20 = 1500
* Ils correspondent aux confirmations d’arrivées des paquets.