Chapitre III Adressage (Couche Internet et Couche Liaison) Partie 3- Internet Control Message Protocol

Ilyas Bambrik

Table des matières

Internet Control Message Protocol (ICMP)

I

- Internet Control Message Protocol (ICMP) est un protocole permettant de diagnostiquer le fonctionnement du réseau et de signaler des erreurs de routage ;
- ICMP fonctionne au niveau de la Couche Internet du modèle TCP / IP ;
- Plusieurs commandes utilisent ICMP pour fonctionner (ping, tracert / traceroute).
- Les messages générés par ce protocole sont encapsulés par un entête IP. Si dans un message IPv4 *la valeu du champs Protocol est égale à 1*, le message encapsulé est un message ICMP ;
- La plus part des machines fonctionnant sur Internet sont configurées pour répondre aux messages ICMP (comme ping par exemple);

Structure du message ICMP

II

- La structure du message ICMP change selon la valeur du champ *type*;
- Les champs suivants qui peuvent être présents dans un message ICMP sont :

1. *Type [présent dans tous les messages ICMP]:* Valeur numérique qui indique le type du message ICMP. Il existe 16 types de messages ICMP mais ceux fréquemment rencontrées sont :
   0—Echo reply
   3—Destination unreachable
   5—Redirect
   8—Echo request
   11—Time Exceeded
2. *Code [présent dans tous les messages ICMP]:* La valeur du code prend souvent 0. Si ce champ prend une valeur différent de 0, cela indique que le message ICMP représente une variation d'un type de message (*champ 1*). Pour les messages ICMP qui n'ont pas de variantes, le champ *code* prends toujours la valeur 0 ;
3. *Checksum [présent dans tous les messages ICMP]:* Valeur de contrôle du message ICMP entier ;
4. *Identifiant* : N'est pas présent dans tous les types de messages ICMP. Cette valeur peut faire référence à un message ICMP précédant qui a provoqué l'envoie de ce message ICMP ;
5. *Numéro de séquence :* Comme l'identifiant, la valeur de ce champ est utilisée pour faire la correspondance entre le *Echo Request* et le *Echo Reply* ;
6. *Copie de l'entête IP + copie de 64 bits des données encapsulées* (8 octets) : Ce champs est présent dans certains types de message ICMP pour faire référence au message qui a provoqué la génération de ce dernier ;
7. *Payload*: Les données enveloppées par le message ICMP ;

Echo Request (Type ==8) et Echo Reply (Type ==0)

III

- La commande *ping* présente sur Windows et Linux génère un message *ICMP Echo Request (Type == 8)* ;
- Le destinataire qui correspond à l'adresse IP fournie répond avec un message *ICMP Echo Reply (Type == 0)*;
- Le payload d'un message Echo Request contient une suite d'octets. Les octets insérés dans ce champ dépendent du système d'exploitation. Par exemple : Windows génère un payload de 32 octets contenant des caractères alphabétiques (de *'a' jusqu'à 'z' et ensuite de 'a' jusqu'à 'i'*), Ubuntu génère une suite de 48 octets avec une suite de caractères différente) ;
- Le Echo Reply correspondant à un Echo Request aura la même valeur d'identification, le même numéro séquence et la même suite d'octets constituant le payload ;

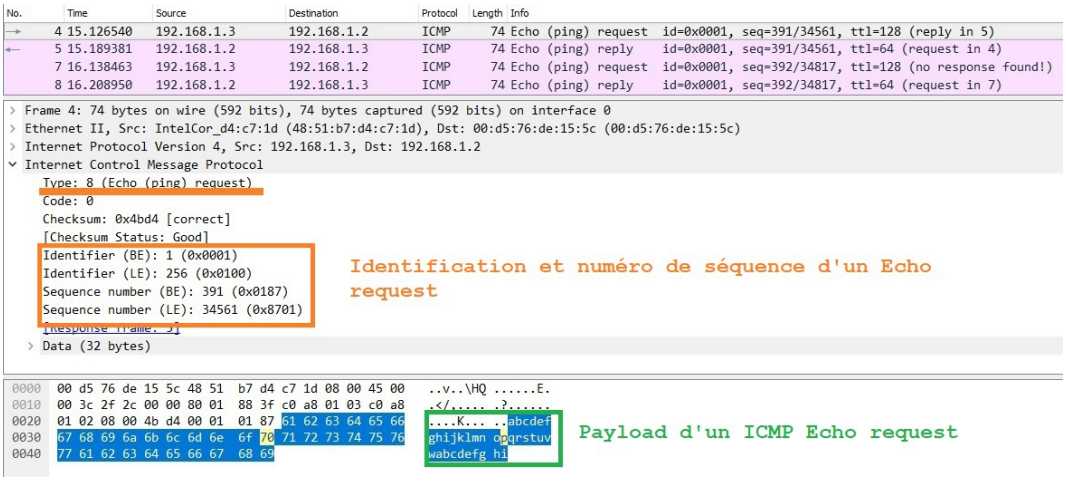

Figure 1. Echo Request

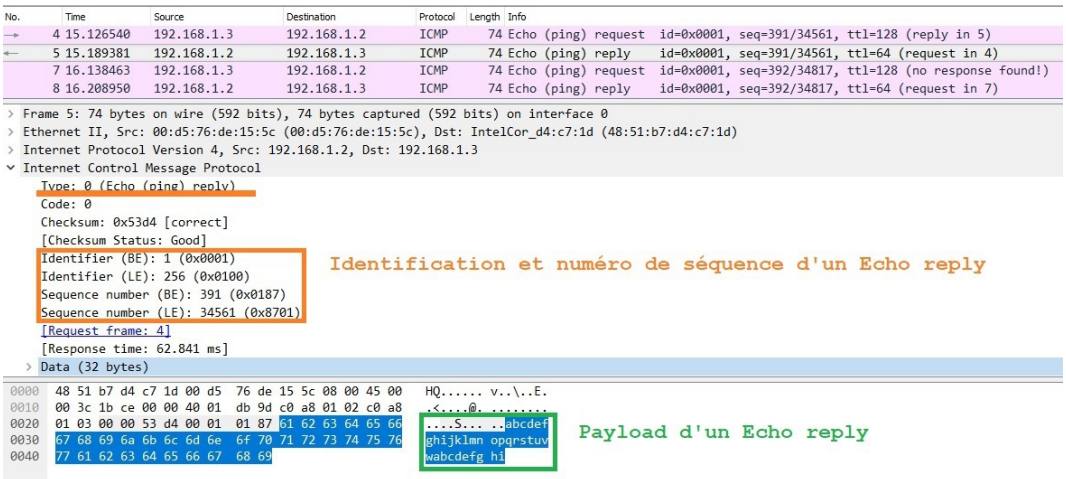

Figure 2. Echo Reply

Remarque : Identification et numéro de séquence

Wireshark affiche l'identification et le numéro de séquence d'un message ICMP sous deux formats (BE == Big Endian , LE == Little Endian).

ICMP Time Exceeded (Type ==11)

IV

- Dans le cas où un paquet encapsulé avec un entête IP est supprimé à cause de l'expiration du TTL (TTL == 0), le routeur qui supprime le paquet transmet un *message ICMP avec Time Exceeded (Type == 11)* vers la source du paquet supprimé ;
- Ceci informe la source que le paquet a potentiellement traversé une boucle de routage (routing loop) ;
- Contrairement à Echo reply / request, un message ICMP Time Exceeded ne contient pas le champ identification / numéro de séquence. Ce type de message contient une copie du message qui a expiré (TTL a atteint 0) ;
- Le deuxième cas d'utilisation pour Time Exceeded c'est lorsque un fragment est perdu/supprimé ainsi le reste des fragments ne peuvent pas être livrés à la couche transport. Dans ce cas, un message *Time Exceeded (Type == 11)* avec code =1 est envoyé (Temps de ré-assemblage des fragments du datagramme dépassé) ;

Remarque : TTL

- Chaque fois qu'un paquet est retransmis par un routeur, la valeur du TTL est décrémentée par au moins 1. Dans certaines situations, le TTL est décrémenté par une valeur supérieure ;
- La commande *Tracert* (traceroute sur Linux) utilise ICMP Time Exceeded pour retrouver les sauts sur le chemin vers la destination. La source transmet des messages *ICMP Echo Request avec des TTL incrémentés* de 1 jusqu'à ce que la source est atteinte. La transmission d'un echo request avec un TTL ==N permet de traverser N sauts seulement (car la machine positionnée dans le saut numéro N supprimera le paquet puisque le TTL initial a été décrémenté N fois au moins pour l'atteindre). Chaque fois qu'une machine sur la route supprime le message à cause de l'expiration du TTL, elle renvoie un ICMP Time Exceeded vers la source. Ainsi, la source détermine le générateur du ICMP Type ==11 est positionnée sur la route à la N^{em} *position* ;
- Lorsque l'administrateur réseau souhaite qu'une machine ne soit pas visible dans la route tracée par cette commande, il suffit de configurer celle-ci pour ne pas décrémenter le TTL

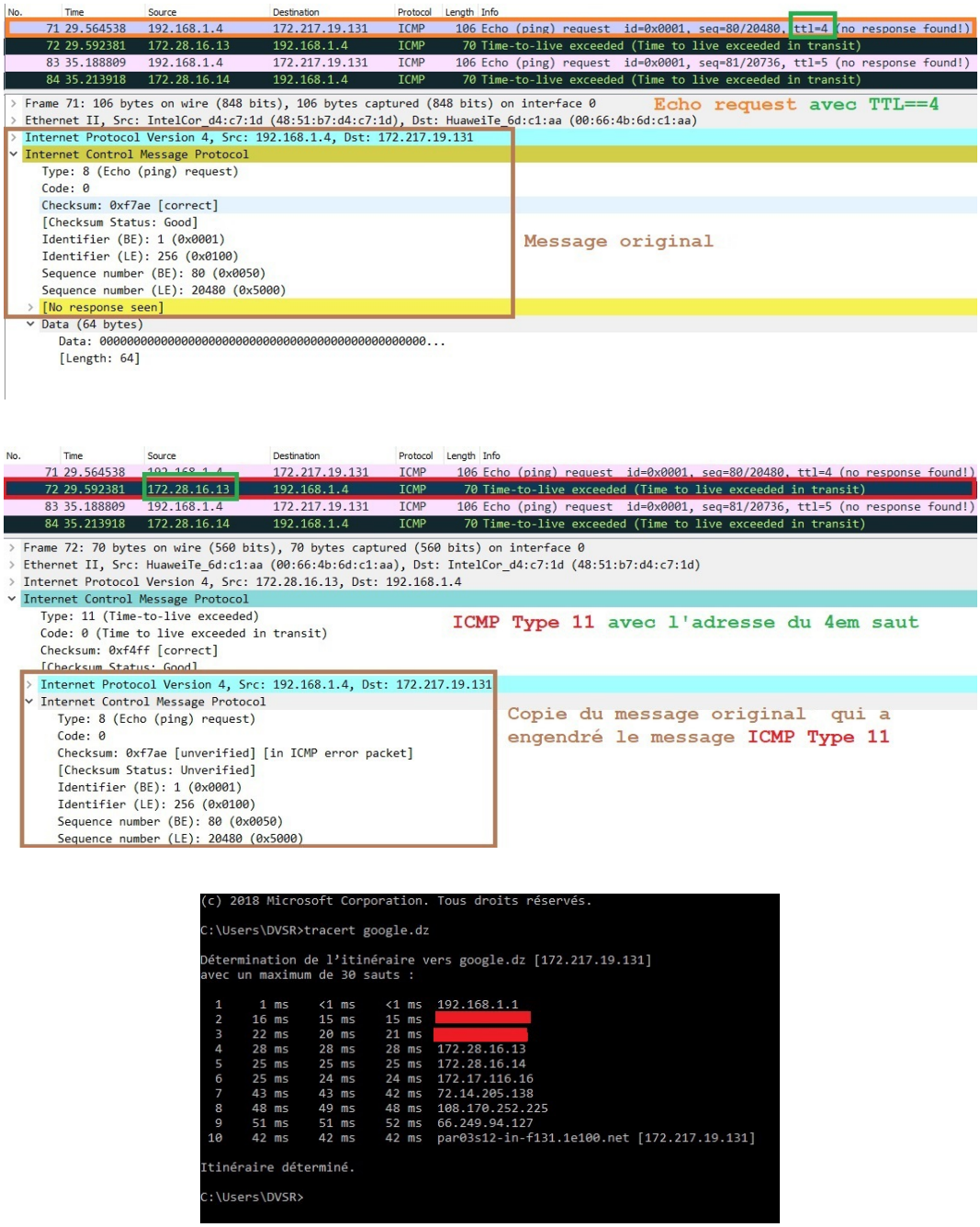

Figure 4. Fonctionnement de la commande Tracert

Exemple : Boucle de routage

Par exemple, Routeur 3 a une route manuellement configurée vers le réseau 192.168.1.0 et Routeur 2 est configuré avec le Routeur 3 comme route par défaut. Si la route vers 192.168.1.0 est supprimée de Routeur 2 à cause d'une panne, lorsque Routeur 3 souhaite communiquer avec 192.168.1.0 , une boucle de routage se formera : car Routeur 3 utilise Routeur 2 pour atteindre 192.168.1.0, et Routeur 2 n'a pas de route vers 192.168.1.0 et donc utilisera la route par défaut (Routeur 3). Ainsi, Routeur 2 et Routeur 3 s'échangeront le message destiné au réseau 192.168.1.0 jusqu'à ce que le TTL du paquet atteindra 0 et un message ICMP Type 11 est transmis vers la source de cette transmission ;

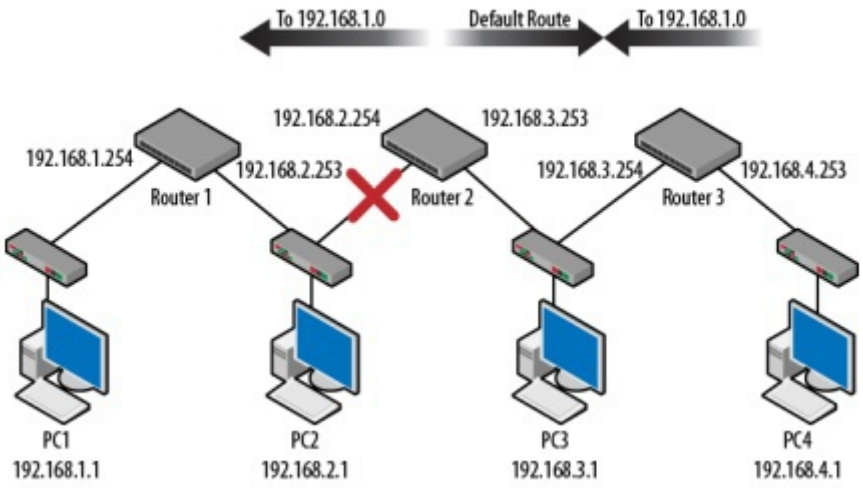

Figure 3. Boucle de routage [*Packet Guide to Core Network Protocols*]

ICMP Destination Unreachable (Type ==3)

V

Un message ICMP de type 3 est généré quand le paquet ne trouve pas une route correspondante à la destination ou ne peut pas être transmis vers celle-ci. Les codes (*variations*) suivants possibles pour ce type de message sont :

0—Net unreachable : Le réseau n'est pas atteignable ;

1—Host unreachable : La machine n'est pas atteignable ;

2—Protocol unreachable : Le protocole de transport utilisé n'est pas supporté ;

3—Port unreachable : La destination n'a pas de service correspondant au numéro de port et il n'y a pas un mécanisme pour informer la source (*comme c'est le cas pour UDP !)*;

4—Fragmentation needed and DF (do not fragment) set : Le paquet ne peut pas être transmis car Do Not Fragment == 1 et la fragmentation a été requise ;

5—Source route failed : Le message original utilise Source Routing et cette option est bloquée par le routeur ;

13—Communication administratively filtered : Le paquet a été bloqué à cause d'un filtre administrative basé sur le contenu (par exemple le firewall [*pare-feu*] est configuré pour bloquer les paquets destinés au port 137) ;

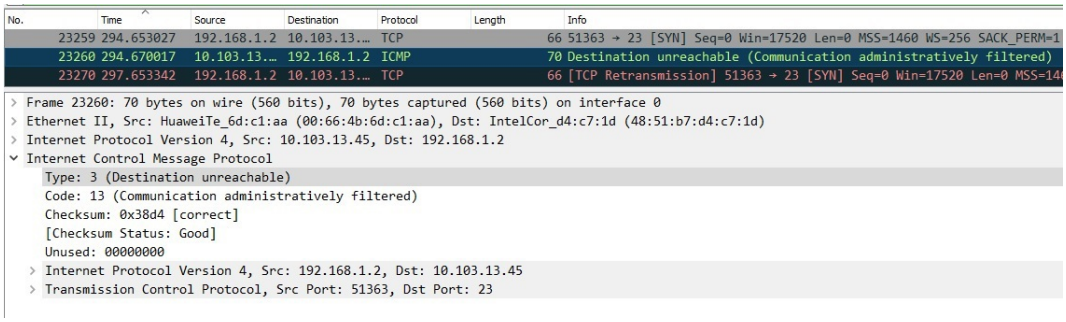

Figure 5. Communication administratively filtered

Chacun de ces messages ICMP type 3 contient une copie de l'entête et du payload [*champ 7 du message ICMP*] du message que le routeur a échoué de livrer.

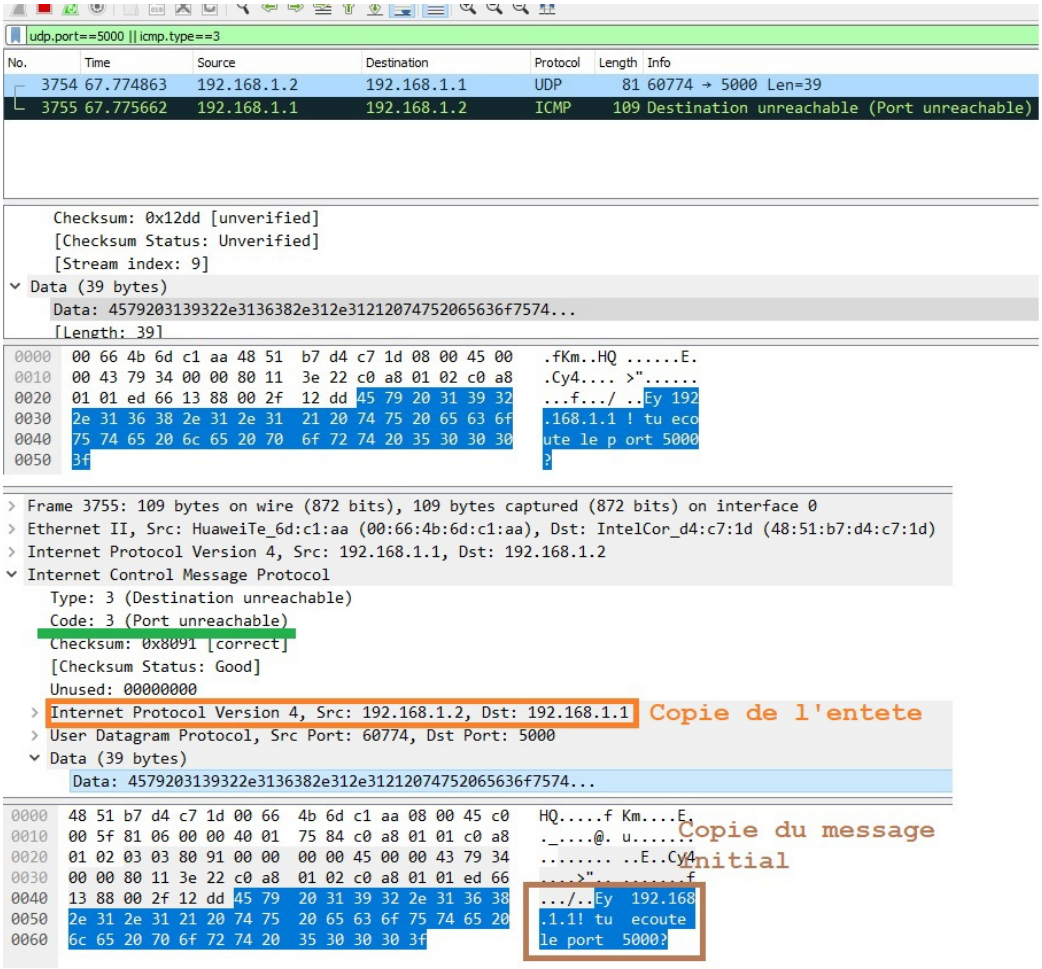

Figure 6. Message ICMP Type ==3 Code ==3

Remarque : Traceroute sur Linux

Alors que tracert sur Windows utilise *echo request* et *ICMP TTL Exeeded,* la commande Traceroute sur Linux génère des *datagrames UDP* avec un TTL progressivement incrémenté et attend de recevoir le message ICMP TTL Exeeded par les machines intermédiaires. La destination finale répondra généralement avec un ICMP Destination Unreachable (Type 3) Port Unreachable (Code 3).

ICMP Redirect (Type ==5)

VI

Un message ICMP Redirect (Type ==5) est généré pour informer la source d'un paquet que ça destination est joignable par un plus court chemin *dans le même réseau*. Ainsi, le routeur qui génère un paquet ICMP Redirect envoie la nouvelle route vers la source. Ensuite, la source ajoute une nouvelle entrée dans ça table de routage vers la destination souhaitée avec le prochain saut égale à la route spécifiée par le ICMP Redirect.

Exemple : Example sénario ICMP Redirect

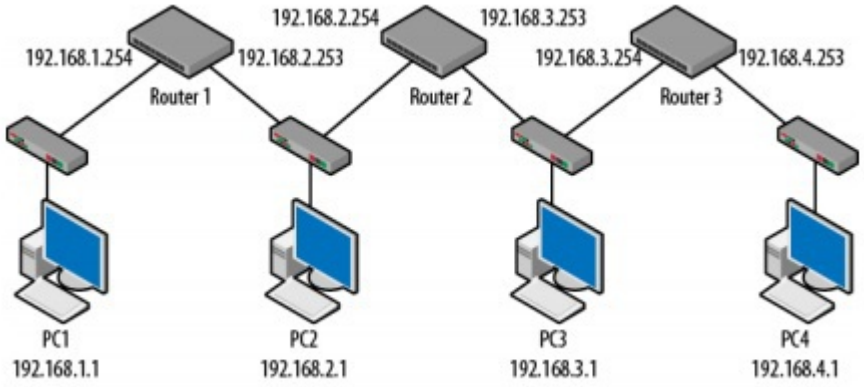

Figure 7. Exemple ICMP Redirect [*Packet Guide to Core Network Protocols*]

- Dans l'exemple présenté dans *Figure 7*, PC3 est configuré avec Routeur 2 comme route par défaut et ne connais pas de route vers le réseau 192.168.4.0 (où PC4 se trouve). En outre, *Routeur 2 connais toutes les routes vers les réseaux atteignables*. Ainsi, quand PC 3 souhaite transmettre des paquets vers PC4, celui-ci utilise Routeur 2.
- Routeur 2 détermine que PC3 possède une route plus courte vers PC4 (car *pour Routeur 2 le prochain sau vers 192.168.4.0 est Routeur 3 && Routeur 3 et PC3 sont dans le même réseau*). Ainsi, *Routeur 2 envoie un message ICMP Redirect vers PC3 pour lui dire qu'il peut rejoindre PC4 à travers Routeur 3* ;

Si *la route est explicitement définie par la source (Source Routing est applqué),* le routeur ne génère pas de ICMP Redirect même s'il y a une meilleur route ;