Le protocole I.C.M.P

1. Rappel sur le protocole IP

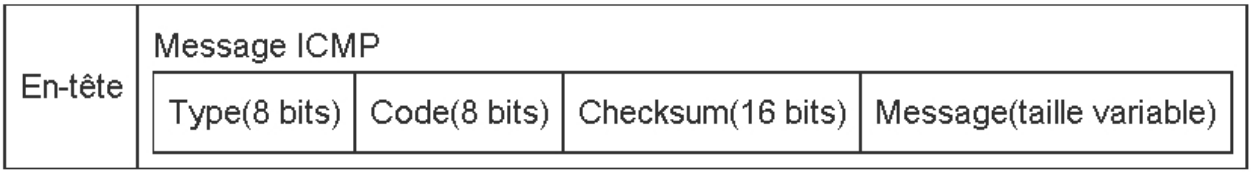
Les données émises sont transmisent par paquets (trames) à l'aide du protocole IP.

- Ce protocole est un protocole qui fonctionne mode "non connecté". Ce protocole est un protocole "non fiable" (les erreurs et les paquets perdus ne sont pas détectées).
- Ce protocole contient (en autre) les adresses de l'ordinateur expéditeur et l'adresse de l'ordinateur récepteur.

2. Protocole I.C.M.P.

Le protocole I.C.M.P. (Internet Control Message Protocol) utilise le protocol IP pour la transmission des trames. Ce protocole à été créé pour controler et gérer les incidents survenant dans le transport de données avec le protocole I.P. Les messages I.C.M.P. Sont transportées dans la partie "DONNEES" de la trame I.P.

Un message "I.C.M.P." peut être émis par le destinataire (*un ordinateur ou un routeur qui reçoivent des trames I.P.*) vers l'émetteur du message "I.P." C'est le protocole "I.P." de la machine "émettrice" qui gére les messages "I.C.M.P." reçues. Ce protocole est nécessaire car sous "I.P", la connexion s'effectue en mode "non connecté".



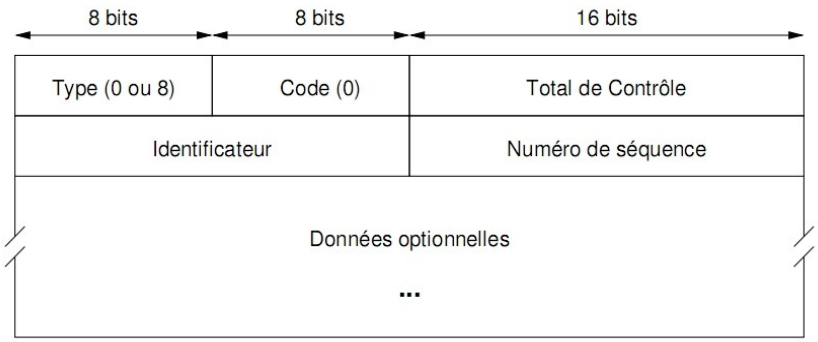
Datagramme Ip contenant un message au format ICMP

Les messages I.C.M.P. émis sont:

Code	Type de message	Traduction
0	Echo reply	Réponse à une demande d'écho
1		Ordinateur inaccessible
2		Protocole inacessible
3	Destination Unreachable	Destination inaccessible
4	Source Quench	Limitation de la production à la source
5	Redirect	Redirection (nouvelle route)
8	Echo request	Demande d'écho
9		Annonce de routeur

Code	Type de message	Traduction
10		Sollicitation de routeur
11	Time Exceeded for a datagram	Expiration de delai pour un datagramme
12	Parameter problem for a datagram	Problème de paramétrage pour un datagramme
13	Timestamp request	Demande d'horodatage
14	Timestamp reply	Réponse à une demande d'horodatage
15		Demande d'informations
16		Réponse à une demande d'informations
17	Address mask request	Demande de masque de sous-réseau
18	Address mask reply	Réponse à une demande de masque de sous-réseau

Exemple: message "Echo reply"



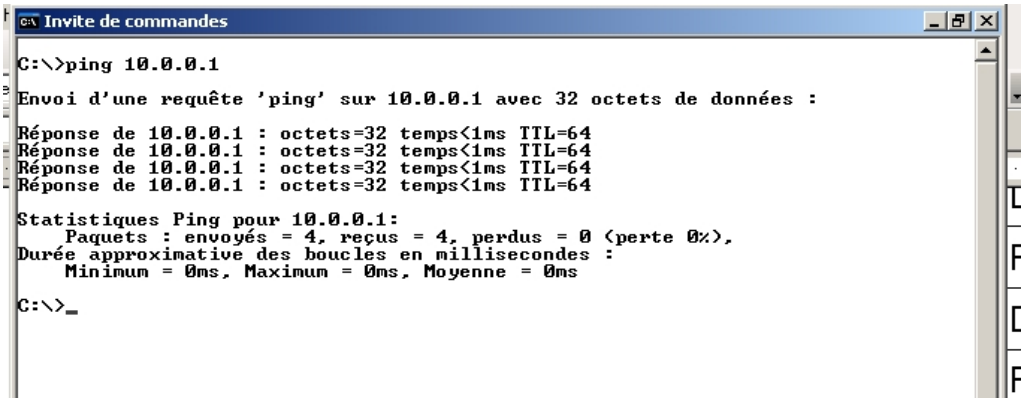
Format du message ICMP d'ECHO

- Type: 8 = demande d'écho 0 = réponse à une demande d'écho
- Code:0
- Total de contrôle:
- Identificateur:zone qui permet d'identifier la machine qui émet le message "Echo reply" (plusieurs machine peuvent faire une demande de test "Echo reply")
- Numéro de séquence:cette zone permet d'ajouter des paramètres à la commande "Echo reply" (nombre "Echo reply" à envoyer, etc.)
- Données optionnelles: cette zone permet de définir des tests supplémentaires par exemple envoi d'un datagramme IP non fragmenté.

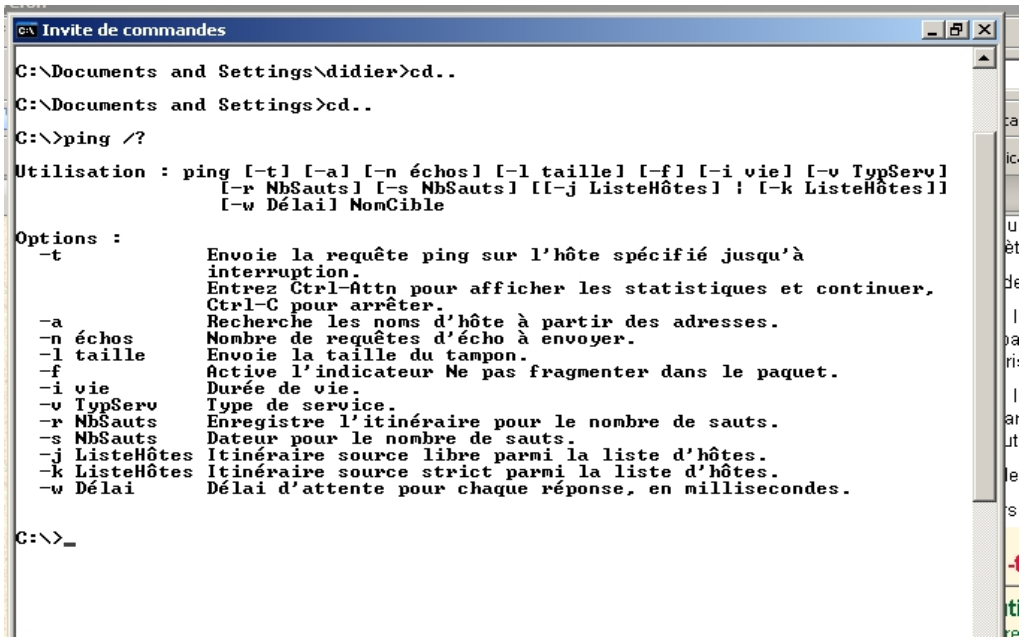
3. La commande "PING"

La commande "PING" (Test d'accessibilité et d'état), qui fonctionne dans une fenêtre de commande "DOS" utilise le protocole I.C.M.P. Avec le message "Echo reply"

ping dans une fenêtre DOS



options de la commande "ping"

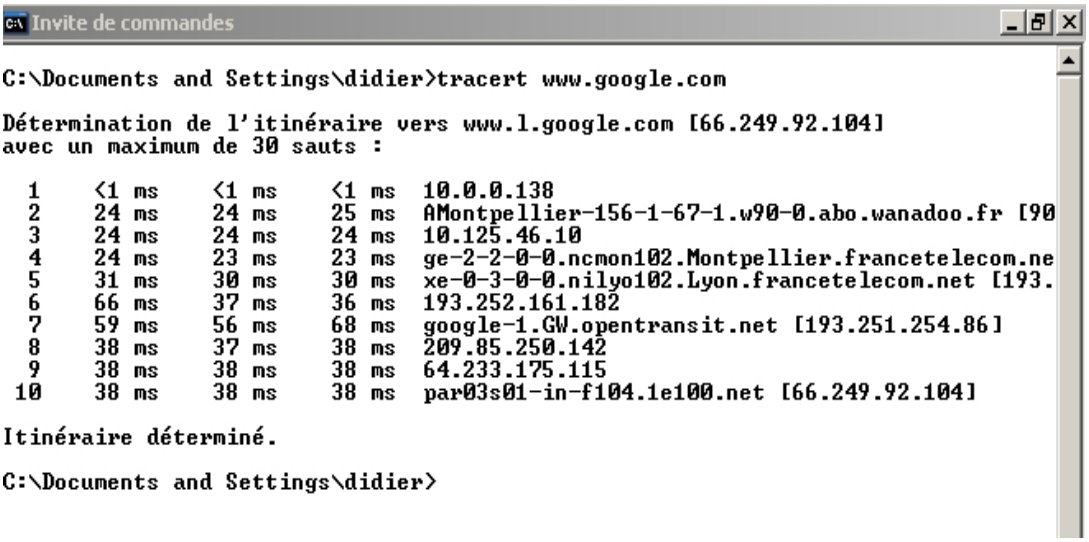


4. La commande "Tracert"

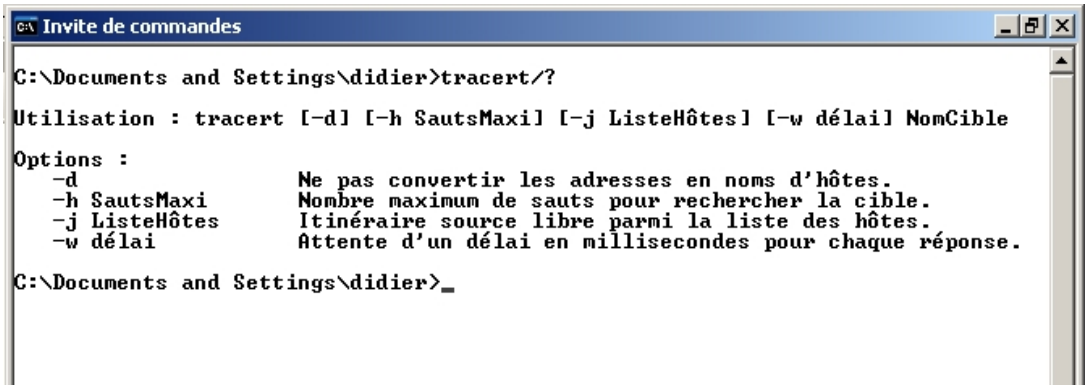
La commande tracert fournit les noms et adresses IP des routeurs successifs trouvés entre l'ordinateur de l'émetteur et l'ordinateur cible. La commande tracert utilise le protocole ICMP.

La commande "Tracert" (Test accessiblité et d'état) qui fonctionne dans une fenêtre de commande "DOS" utilise le protocole I.C.M.P.

Utilisation de l'utilitaire "Tracert"



options de commande "Tracert"



5. Conclusion

Le protocole ICMP à été créé pour contrôler et gérer les incidents survenant dans le transport de données avec le protocole I.P.

Cependant deux utilitaires utilisent ce protocole. L'utilitaire "Ping" permet de tester et de valider la connection matérielle entre deux adresses IP. L'utilitaire "Tracert" affiche la route empreintée (c'est à dire les adresses IP des routeurs utilisées) par les datagrammes entre la machine émettrice et la machine destinatrice des datagrammes.

Note: des logiciels et des sites web fournissent les adresses géographiques des routeurs utilisées.