Septembre 1981

Remplace: RFCs 777, 760
Remplace: IENs 109, 128

INTERNET CONTROL MESSAGE PROTOCOL SPECIFICATION

Table des matières

Introduction

Le Protocole Internet (IP) [1] est utilisé pour la transmission de datagrammes de hôte à hôte à l'intérieur d'un système de réseaux interconnectés appelé Catenet [2]. Les appareils raccordant les réseaux entre eux sont appelés des Routeurs. Ces routeurs communiquent entre eux en utilisant le protocole Routeur à Routeur (GGP) [3,4] afin d'échanger des informations de contrôle et de gestion du réseau. Occasionnellement, un routeur ou un hôte destinataire peut avoir à communiquer vers l'émetteur du datagramme, par exemple, pour signaler une erreur de traitement du datagramme. C'est dans cette perspective qu'a été mis en place le protocole Internet

Control Message Protocol (ICMP). Il s'appuie sur le support de base fourni par IP comme s'il s'agissait d'un protocole d'une couche supérieure. ICMP n'en reste pas moins une partie intégrante du protocole IP, et doit de ce fait être implémenté dans chaque module IP.

Les messages ICMP sont envoyés dans diverses situations: par exemple, lorsqu'un datagramme ne peut pas atteindre sa destination, lorsque le routeur manque de réserve de mémoire pour retransmettre correctement le datagramme, ou lorsque le routeur décode de viser l'hôte destinataire via une route alternative pour optimiser le trafic.

Le protocole Internet n'est pas, dans sa définition, absolument fiable. Le but de ces messages de contrôle est de pouvoir signaler l'apparition d'un cas d'erreur dans l'environnement IP, pas de rendre IP fiable. Aucune garantie que le datagramme soit acheminé ni qu'un message de contrôle soit retourné, de peut être donnée. Certains datagrammes pourront se perdre dans le réseau sans qu'aucun message de contrôle ne le signale. Les protocoles de niveau supérieur s'appuyant sur une couche IP devront implémenter leurs propres mécanismes de contrôle d'erreur et de retransmission si leur objet nécessite un circuit de communication sécurisé.

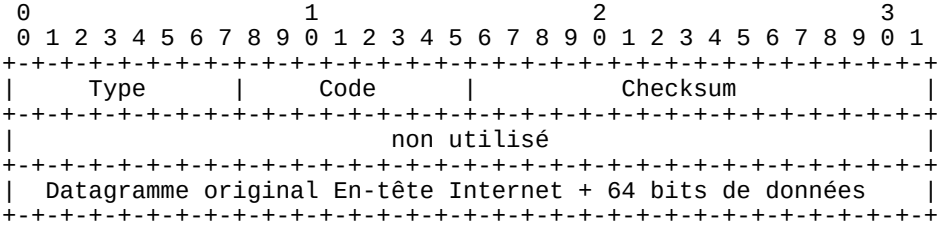
Les messages ICMP reportent principalement des erreurs concernant le traitement d'un datagramme dans un module IP. Pour éviter de ne pas entrer dans un cercle vicieux de réémission de message de contrôle en réponse à un autre message de contrôle et ce sans fin, aucun message ICMP ne sera réémis en réponse à un message ICMP. De même les messages ICMP ne seront transmis qu'en réponse à un traitement erroné du fragment zéro dans le cas d'un datagramme fragmenté. (Le fragment zéro est celui dont l'offset vaut zéro).

Formats de message

Les messages ICMP sont émis en utilisant l'en-tête IP de base. Le premier octet de la section de données du datagramme est le champ de type ICMP; Sa valeur détermine le format du reste des données dans le datagramme ICMP. Tout champ qualifié de "non utilisé" est réservé pour application future et doit être laissé à zéro lors de l'émission, les récepteurs ne DEVANT PAS utiliser ces champs (sauf lorsqu'il s'agit de calculer le Checksum). Sauf mention particulière contraire signalée dans chaque description de message spécifique, les valeurs des champs d'en-tête Internet auront la signification suivante:

Version :	4
IHL :	Longueur d'en-tête Internet en mots de 32-bits.
Type de Service :	0
Longueur Totale :	Longueur totale du datagramme en octets.
Identification :	|
Bits Contrôles :	| Utilisés par le mécanisme de fragmentation, voir [1].
Fragment Offset :	|
Durée de vie :	Durée de vie du datagramme en secondes; ce champ est diminué d'une unité par chaque module IP traversé dans lesquels le datagramme est traité, la valeur dans ce champ doit être au moins égale au nombre maximum de routeurs que ce datagramme est sensé traverser jusqu'à sa destination finale.
Protocole :	ICMP = 1
Checksum :	Le complément à un sur 16 bits de la somme des compléments à un de l'en-tête Internet pris par mots de 16 bits. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Ce mécanisme de Checksum sera changé dans le futur.
Adresse source :	L'adresse du routeur ou hôte qui compose le message ICMP. Sauf mention contraire, celle-ci peut être toute adresse de routeur.
Adresse destinataire :	L'adresse du routeur ou hôte à qui le message doit être envoyé.

Message "destinataire non accessible"



Champs IP:

Adresse destinataire :	L'adresse et réseau source du datagramme original.

Champs ICMP:

Type :	3
Code :	0 = réseau inaccessible; 1 = hôte inaccessible; 2 = protocole non disponible; 3 = port non accessible; 4 = fragmentation nécessaire mais interdite; 5 = échec d'acheminement source.
Checksum :	Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Ce mécanisme de Checksum sera changé dans le futur.

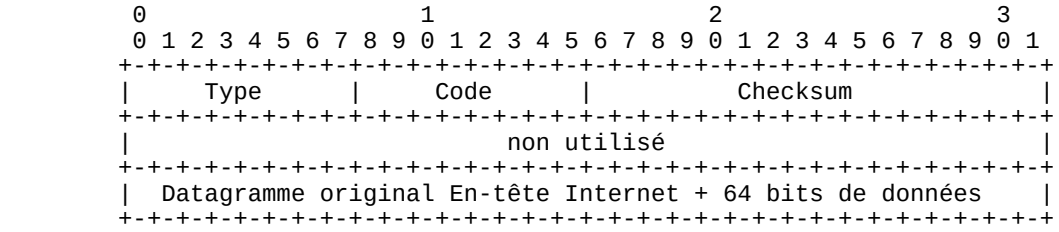
Datagramme avec une en-tête Internet + 64 bits de données

L'en-tête Internet plus les 64 premiers bits extraits du datagramme original. Ces données seront utilisées par l'hôte pour reconnaître le programme concerné par ce message. Si un protocole de niveau supérieur utilise des "numéros de port", on admet que ce dernier apparaît dans les 64 premiers bits de données du datagramme original.

Description

Si, compte tenu des information contenues dans les tables de routage du routeur, le réseau indiqué dans le champ adresse de destination de l'en-tête IP du datagramme reçu est inaccessible ou inconu, ex., la distance à ce réseau est marquée comme infinie, le routeur pourra émettre un tel message a destination de l'hôte d'origine du datagramme. De plus, dans certains réseaux, le routeur peut être capable de déterminer que l'hôte destinataire n'est pas accessible. Un tel routeur pourra, sur réception d'un datagramme destiné à cet hôte, émettre en retour un tel message ICMP, et détruire le datagramme.
Si, dans l'hôte destinataire, le module IP ne peut délivrer le message à la couche supérieure soit parce que le protocole indiqué n'est pas implémenté soit parce que l'application ne répond pas, l'hôte destinataire lui-même peut être amené à émettre un tel message à destination de la source.
Un autre cas de figure est celui où le datagramme doit être fragmenté pour pouvoir être retransmis sur le segment suivant de réseau et où celui-ci affiche un bit antifragmentation marqué interdisant d'effectuer cette opération pour ce datagramme. Ce message ICMP permet de signaler ce cas de figure.
Les codes 0, 1, 4, et 5 seront reçus de la part de routeurs. Les codes 2 et 3 proviendront d'hôtes.

Message "Durée de vie écoulée"



Champs IP :

Adresse destinataire :	L'adresse et réseau source du datagramme original.

Champs ICMP :

Type :	11
Code :	0 = durée de vie écoulée avant arrivée à destination; 1 = temps limite de réassemblage du fragment dépassé.
Checksum :	Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Ce mécanisme de Checksum sera changé dans le futur.

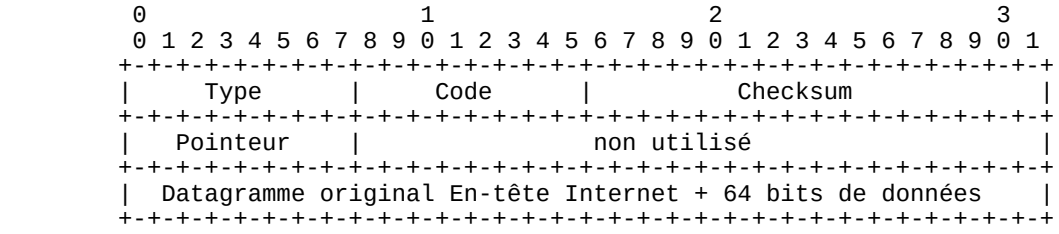
Datagramme avec une en-tête Internet + 64 bits de données

L'en-tête Internet plus les 64 premiers bits extraits du datagramme original. Ces données seront utilisées par l'hôte pour reconnaître le programme concerné par ce message. Si un protocole de niveau supérieur utilise des "numéros de port", on admet que ce dernier apparaît dans les 64 premiers bits de données du datagramme original.

Description

Lorsqu'un routeur traitant un datagramme est amené à mettre à jour le champ Durée de Vie de l'en-tête IP et que ce champ atteint une valeur zéro, le datagramme doit être détruit. Le routeur peut alors prévenir l'hôte source de cette destruction par ce message.
Si un hôte réassemblant un datagramme fragmenté ne peut terminer cette opération à cause de fragments manquants au bout de la temporisation de réassemblage, il doit détruire le datagramme en cours de traitement et peut dans ce cas en avertir la source en émettant ce message.
Si parmi les fragments reçu, aucun ne porte le numéro 0, il n'est pas utile d'envoyer ce message.
Un message de code 0 pourra provenir d'un routeur. Un message de code 1 peut être reçu provenant d'un hôte.

Message d'erreur de paramètre



Champs IP :

Adresse destinataire : L'adresse et réseau source du datagramme original.

Champs ICMP :

Type : 12
Code : 0 = l'erreur est indiquée par le pointeur.
Checksum : Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Ce mécanisme de Checksum sera changé dans le futur.
Pointer : Si code = 0, identifie l'octet où l'erreur a été détectée.

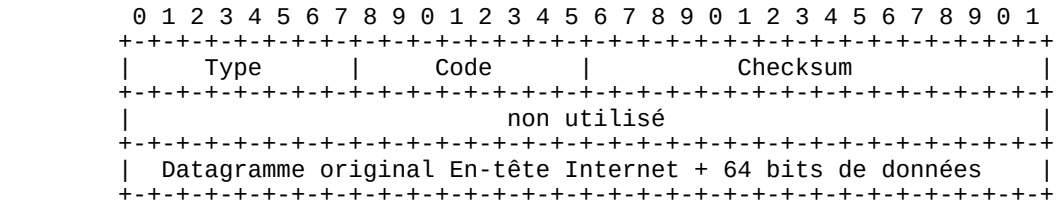
Datagramme avec une en-tête Internet + 64 bits de données

L'en-tête Internet plus les 64 premiers bits extraits du datagramme original. Ces données seront utilisées par l'hôte pour reconnaître le programme concerné par ce message. Si un protocole de niveau supérieur utilise des "numéros de port", on admet que ce dernier apparaît dans les 64 premiers bits de données du datagramme original.

Description

Si le routeur où l'hôte traitant le datagramme rencontre un problème avec un paramètre d'en-tête l'empêchant de finir son traitement, le datagramme doit être détruit. Un exemple possible pour ce cas est la présence d'arguments invalides dans une option. Le routeur ou l'hôte détectant la faute peut alors en avertir la source par un tel message. Cependant, un tel message ne peut être envoyé que si la faute est de nature à empêcher le traitement du datagramme.
Le pointeur identifie l'octet par sa position dans l'en-tête du datagramme original dans laquelle l'erreur a été détectée (cela peut être au milieu d'une option). Par exemple, une valeur de 1 indique un Type de Service erroné, et (si l'en-tête comporte des options) 20 indique une erreur sur le code de type de la première option.
Un message de code 0 pourront provenir d'un routeur ou d'un hôte.

Message de contrôle de flux



Champs IP :

Adresse destinataire : L'adresse et réseau source du datagramme original.

Champs ICMP :

Type : 4
Code : 0
Checksum : Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Ce mécanisme de Checksum sera changé dans le futur.

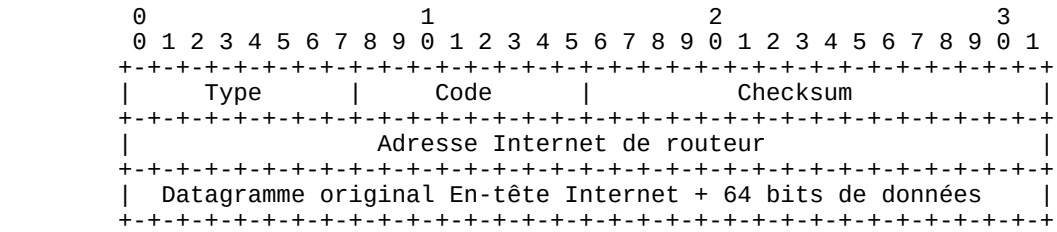
Datagramme avec une en-tête Internet + 64 bits de données

L'en-tête Internet plus les 64 premiers bits extraits du datagramme original. Ces données seront utilisées par l'hôte pour reconnaître le programme concerné par ce message. Si un protocole de niveau supérieur utilise des "numéros de port", on admet que ce dernier apparaît dans les 64 premiers bits de données du datagramme original.

Description

Un routeur peut être amené à détruire un datagramme s'il manque de mémoire pour tamponner les datagrammes à émettre sur le segment de réseau suivant du chemin d'acheminement. Dans ce cas, il pourra émettre ce message à destination de la source du datagramme détruit. Un hôte destinataire peut aussi émettre ce message si le datagramme arrive trop rapidement pour qu'il puisse être traité. Ce message peut donc constituer une demande à la source de diminuer le débit d'émission de données vers le destinataire. Le routeur devra émettre autant de messages de ce type que de datagrammes détruits. Sur réception de ce message, l'hôte source devra faire chuter son débit d'émission vers cette destination tant que de tels messages lui parviennent. L'hôte source pourra alors graduellement augmenter son débit de sortie jusqu'à de nouveau recevoir ce type de message.
Il sera plus judicieux de faire émettre ce message lorsque les ressources du routeur ou de l'hôte passent en dessous d'une valeur de sécurité, plutôt que d'attendre de ne plus disposer de ressource du tout. Ceci veut aussi dire que le datagramme ayant déclenché l'émission de ce message aura de fortes chances d'arriver quand même à destination.
Le message de code 0 pourront provenir d'un hôte ou d'un routeur.

Message de redirection



Champs IP :

Adresse destinataire : L'adresse et réseau source du datagramme original.

Champs ICMP :

Type : 5
Code : 0 = Redirection de datagramme sur la base du réseau.
1 = Redirection de datagramme sur la base de l'adresse d'hôte.
2 = Redirection de datagramme sur la base du réseau et du Type de Service.

3 = Redirection de datagramme sur la base de l'hôte et du Type de Service.

Checksum : Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Ce mécanisme de Checksum sera changé dans le futur.

Adresse Internet de routeur : Adresse du routeur auquel le trafic à destination du réseau spécifié dans le champ de destination de l'en-tête IP du datagramme original doit être envoyé.

Datagramme avec une en-tête Internet + 64 bits de données

L'en-tête Internet plus les 64 premiers bits extraits du datagramme original. Ces données seront utilisées par l'hôte pour reconnaître le programme concerné par ce message. Si un protocole de niveau supérieur utilise des "numéros de port", on admet que ce dernier apparaît dans les 64 premiers bits de données du datagramme original.

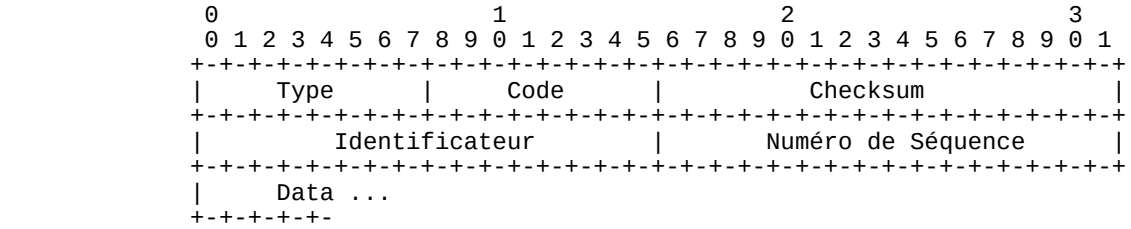
Description

Un routeur peut rediriger un datagramme destiné à un hôte dans les situations suivantes. Un routeur, G1, reçoit un datagramme Internet en provenance d'un hôte situé sur le segment local de réseau où il se trouve. Le routeur, G1, vérifie ses tables de routage et obtient l'adresse du routeur suivant, G2, situé sur le chemin d'acheminement de ce datagramme vers le réseau local destinataire, X. Si G2 et l'hôte source se trouvent être sur le même segment de réseau, un message de redirection est envoyé vers l'hôte source. Il permet d'avertir la source que le trafic vers le réseau X peut être directement adressé au routeur G2, diminuant ainsi le chemin d'acheminement. Le routeur reportera le datagramme original vers sa destination Internet.

Pour les datagrammes présentant une option IP de routage précisant l'adresse du routeur dans le champ de destination, aucun message de redirection ne sera émis même si un chemin plus court vers la destination finale existe, autre que celui indiqué par l'adresse suivante de la liste de routage.

Les messages de codes 0, 1, 2, et 3 pourront provenir d'un routeur.

Message d'écho et de "réponse à écho"



Champs IP :

Adresses : L'adresse de la source dans un message d'écho doit être le destinataire du message de "réponse à écho". Pour constituer un message de réponse à écho, il suffit d'inverser les adresses de source et de destination, et de mettre code type à 0, puis enfin de recalculer le Checksum.

Champs ICMP :

Type : 8 = écho;
0 = réponse à écho.

Code : 0

Checksum : Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Si la longueur totale du message est un nombre impair d'octets, le calcul du Checksum se fera en ajoutant un dernier octet à zéro de bourrage en fin de message. Ce mécanisme de Checksum sera changé dans le futur.

Identificateur : Si le code = 0, un identificateur permettant d'associer l'écho et la réponse à l'écho, peut être nul.

Numéro de séquence : Si le code = 0, un numéro de séquence permettant d'associer l'écho et sa réponse. Peut être nul

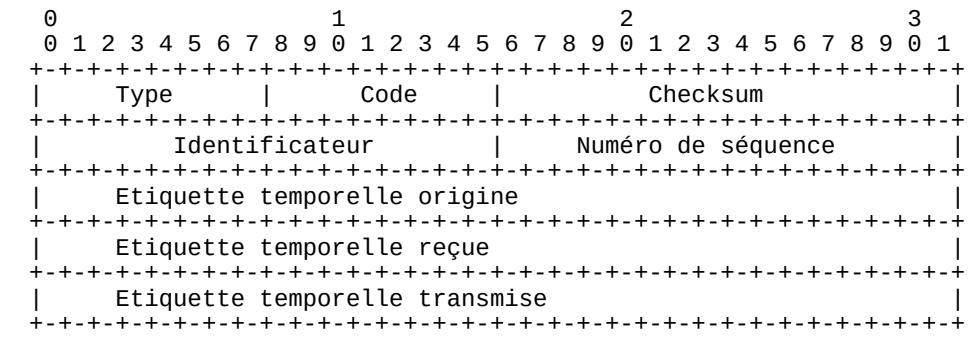
Description

Les données reçues dans un message d'écho doivent être réémises dans la réponse à l'écho.

L'identificateur et le numéro de séquence peuvent être utilisés par l'émetteur du message d'écho afin d'associer facilement l'écho et sa réponse. Par exemple, l'identificateur peut être utilisé comme l'est un port pour TCP ou UDP, identifiant ainsi une session, et le numéro de séquence incrémenté pour chaque message d'écho envoyé. Le "miroir" respectera ces deux valeurs pour renvoyer le retour.

Les messages de code 0 peuvent provenir d'un routeur ou d'un hôte.

Marqueur temporel ou réponse à marqueur temporel



Champs IP :

Adresses :	L'adresse source dans un marqueur temporel doit être la destination du message de réponse à marqueur temporel. Pour constituer une telle réponse, on intervertira simplement l'adresse source et l'adresse de destination, on marquera le code de type à la valeur 14, et le Checksum sera recalculé.

Champs ICMP :

Type :	13 = marqueur temporel; 14 = réponse à marqueur temporel.
Code :	0
Checksum :	Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Ce mécanisme de Checksum sera changé dans le futur.
Identificateur :	Si le code = 0, un identificateur permettant d'associer le marqueur et sa réponse, peut être nul.
Numéro de séquence :	Si le code = 0, un numéro de séquence permettant d'associer le marqueur et sa réponse. Peut être nul

Description

Les données reçues (une étiquette temporelle) dans le message sont recopiées dans la réponse, additionnées d'une étiquette supplémentaire. Une étiquette temporelle code une durée en millisecondes sur 32 bits à partir de minuit GMT. Une utilisation de ces étiquettes temporelles est décrite par Mills [5].

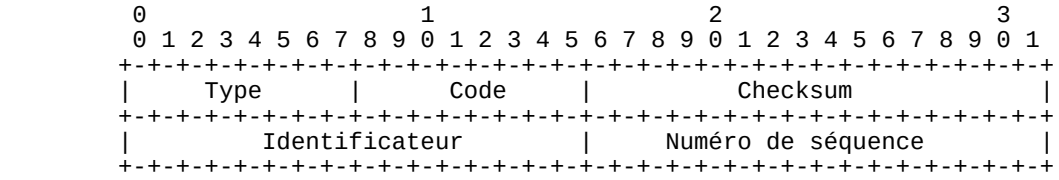
L'étiquette Origine est l'heure à laquelle le message a été modifié pour la dernière fois par la source avant de l'envoyer, L'étiquette de Réception donne l'heure à laquelle la cible a reçu le message, et l'étiquette de Transmission donne l'heure à laquelle la cible réémet le message.

Si l'heure ne peut être obtenue en millisecondes ou ne peut être calculée par rapport à la référence 0 h 00 GMT, alors toute heure peut être codée dans l'étiquette temporelle pourvu que le bit de poids fort soit marqué pour indiquer la présence d'une valeur non standard.

L'identificateur et le numéro de séquence peuvent être utilisés par l'émetteur du marqueur temporel afin d'associer facilement le marqueur et sa réponse. Par exemple, l'identificateur peut être utilisé comme l'est un port pour TCP ou UDP, identifiant ainsi une session, et le numéro de séquence incrémenté pour chaque marqueur envoyé. Le "miroir" respectera ces deux valeurs pour renvoyer le retour.

Les messages de code 0 peuvent provenir d'un routeur ou d'un hôte.

Messages Demande d'Information et Réponse



Champs IP :

Adresses :	L'adresse source dans un message d'information doit être la destination du message de réponse à demande d'information. Pour constituer une telle réponse, on intervertira simplement l'adresse source et l'adresse de destination, on marquera le code de type à la valeur 16, et le Checksum sera recalculé.

Champs ICMP :

Type :	15 = demande d'information; 16 = réponse.
Code :	0
Checksum :	Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Ce mécanisme de Checksum sera changé dans le futur.
Identificateur :	Si le code = 0, un identificateur permettant d'associer la demande et sa réponse, peut être nul.
Numéro de séquence :	Si le code = 0, un numéro de séquence permettant d'associer la demande et sa réponse. Peut être nul

Description

Ce message peut être envoyé vers une adresse constituée du numéro de réseau dans le champ source de l'en-tête IP et un champ destinataire à 0 (ce qui signifie "ce" réseau). Le module IP qui répondra pourra alors envoyer une réponse avec les adresses entièrement renseignées. Par ce message, un hôte peut demander à un routeur le numéro du réseau sur lequel il est situé.

L'identificateur et le numéro de séquence peuvent être utilisés par l'émetteur du message de demande d'information afin d'associer facilement la demande et sa réponse. Par exemple, l'identificateur peut être utilisé comme l'est un port pour TCP ou UDP, identifiant ainsi une session, et le numéro de séquence incrémenté pour chaque message de demande d'information envoyé. Le "miroir" respectera ces deux valeurs pour renvoyer le retour.

Les messages de code 0 peuvent provenir d'un routeur ou d'un hôte.

Résumé des types de Message

0 Réponse Echo
3 Destination non accessible
4 Contrôle de flux
5 Redirection
8 Echo
11 Durée de vie écoulée
12 Erreur de Paramètre
13 Marqueur temporelle
14 Réponse à marqueur temporel
15 Demande d'information
16 Réponse à demande d'information

Références

[1] Postel, J. (ed.), "Internet Protocol - DARPA Internet Program Protocol Specification," RFC 791, USC/Information Sciences Institute, September 1981.

[2] Cerf, V., "The Catenet Model for Internetworking," IEN 48, Information Processing Techniques Office, Defense Advanced Research Projects Agency, July 1978.

[3] Strazisar, V., "Gateway Routing: An Implementation Specification", IEN 30, Bolt Beranek and Newman, April 1979.

[4] Strazisar, V., "How to Build a Gateway", IEN 109, Bolt Beranek and Newman, August 1979.

[5] Mills, D., "DCNET Internet Clock Service," RFC 778, COMSAT Laboratories, April 1981.