

Groupe de travail Réseau

Request for Comments : 0792

RFC mises à jour : RFC 777, 760

IEN mises à jour : IEN 109, IEN 128

J. Postel, ISI

septembre 1981

Spécification du protocole de message de contrôle Internet

Table des matières

1. Introduction.....	2
2. Formats de message.....	2
3. Message Destination injoignable.....	3
Champs IP :	3
Champs ICMP :	3
Description.....	3
4. Message Durée de vie écoulée.....	4
Champs IP :	4
Champs ICMP :	4
Description.....	4
5. Message Problème de paramètre.....	4
Champs IP :	5
Champs ICMP :	5
Description.....	5
6. Message Extinction de source.....	5
Champs IP :	5
Champs ICMP :	5
Description.....	6
7. Message Redirection.....	6
Champs IP :	6
Champs ICMP :	6
Description.....	6
8. Message Écho et Réponse d'écho.....	7
Champs IP :	7
Champs ICMP :	7
Description.....	7
9. Message Horodatage ou Réponse d'horodatage.....	7
Champs IP :	8
Champs ICMP :	8
Description.....	8
10. Message Demande d'Informations ou Réponse d'informations.....	8
Champs IP :	8
Champs ICMP :	8
Description.....	9
11. Résumé des types de Message.....	9
12. Références.....	9

1. Introduction

Le Protocole Internet (IP) [RFC0791] est utilisé pour la transmission de datagrammes d'hôte à hôte à l'intérieur d'un système de réseaux interconnectés appelé Catenet [IEN48]. Les appareils raccordant les réseaux entre eux sont appelés des routeurs. Ces routeurs communiquent entre eux en utilisant le protocole Routeur à Routeur (GGP) [IEN30], [IEN109] afin d'échanger des informations de contrôle et de gestion du réseau. Occasionnellement, un routeur ou un hôte destinataire peut avoir à communiquer avec un hôte se source, par exemple, pour signaler une erreur de traitement du datagramme. C'est dans cette perspective qu'a été mis en place le protocole de message de contrôle Internet (ICMP, *Internet Control Message Protocol*). 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 mis en œuvre 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 peut conduire l'hôte à envoyer le trafic sur un plus court chemin.

Le protocole Internet n'est pas conçu pour être absolument fiable. Le but de ces messages de contrôle est de fournir des retours sur les problèmes dans l'environnement de communication, pas de rendre IP fiable. Aucune garantie que le datagramme soit livré ni qu'un message de contrôle soit retourné, ne peut être donnée. Certains datagrammes peuvent encore n'être pas livrés sans aucun rapport de leur perte. Les protocoles de niveau supérieur qui utilisent IP doivent mettre en œuvre leurs propres procédures de fiabilité si ils nécessitent une communication fiable.

Les messages ICMP reportent normalement les erreurs de traitement des datagrammes. Pour éviter d'entrer dans un cercle vicieux de réémission sans fin de messages de contrôle en réponse à un autre message de contrôle, aucun message ICMP n'est émis en réponse à un message ICMP. De même les messages ICMP ne sont émis que sur des erreurs de traitement du fragment zéro des datagrammes fragmentés. (Le fragment zéro est celui dont le décalage de fragment vaut zéro).

2. Formats de message

Les messages ICMP sont envoyés en utilisant l'en-tête IP de base. Le premier octet de la portion de données du datagramme est le champ de type ICMP ; la valeur de ce champ détermine le format du reste des données. Tout champ qualifié de "non utilisé" est réservé pour des extensions futures et doit être à zéro à l'émission, mais les receveurs ne devraient pas utiliser ces champs (sauf pour les inclure dans la somme de contrôle). Sauf mention contraire notée dans les description de format individuelles, les valeurs des champs d'en-tête Internet sont les suivantes :

Version : 4

IHL : Longueur de l'en-tête Internet et données en octets.

Type de Service :

Longueur Totale : Longueur totale du datagramme en octets.

Identification, fanions, décalage de fragment : Utilisés par le mécanisme de fragmentation, voir [RFC0791].

Durée de vie : Durée de vie en secondes ; comme ce champ est décrémenté à chaque machine où le datagramme est traité, la valeur dans ce champ devrait être au moins égale au nombre de routeurs que ce datagramme va traverser.

Protocole : ICMP = 1

Somme de contrôle d'en-tête : complément à un sur 16 bits de la somme des compléments à un de tous les mots de 16 bits de l'en-tête. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être à zéro. Cette somme de contrôle pourra être changée à l'avenir.

Adresse de source : adresse du routeur ou hôte qui compose le message ICMP. Sauf mention contraire, ce peut être n'importe quelle adresse du routeur.

Adresse destinataire : L'adresse du routeur ou hôte à qui le message devrait être envoyé.

3. Message Destination injoignable

```

0           1           2           3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Type           |           Code           |           Somme de contrôle           |
+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     non utilisé                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
| En-tête Internet + 64 bits de données du datagramme original |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Champs IP:

Adresse de destination : réseau et adresse de source des données du datagramme original.

Champs ICMP :

Type : 3

Code : 0 = réseau injoignable ;

1 = hôte injoignable ;

- 2 = protocole injoignable ;
- 3 = accès injoignable ;
- 4 = fragmentation nécessaire et bit DF établi
- 5 = échec d'acheminement de source.

Somme de contrôle : Le complément à un sur 16 bits de la somme des compléments à un du message ICMP en commençant par le type ICMP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être à zéro. Cette somme de contrôle pourra être changée à l'avenir.

En-tête Internet + 64 bits de datagramme de données : L'en-tête Internet plus les 64 premiers bits des données du datagramme original. Ces données sont utilisées par l'hôte pour confronter le message au processus approprié. Si un protocole de niveau supérieur utilise des numéros d'accès, ils sont supposés être dans les 64 premiers bits des données du datagramme original.

Description

Si, compte tenu des informations contenues dans les tableaux d'acheminement du routeur, le réseau indiqué dans le champ Adresse de destination Internet d'un datagramme est injoignable, par exemple, la distance à ce réseau est infinie, le routeur peut envoyer un message Destination injoignable à l'hôte d'origine du datagramme. De plus, dans certains réseaux, le routeur peut être capable de déterminer si l'hôte de destination Internet est injoignable. Les routeurs dans ces réseaux peuvent envoyer des messages Destination injoignable à l'hôte de source quand l'hôte de destination est injoignable.

Si, chez l'hôte de destination, le module IP ne peut livrer le message parce que le module ou processus de protocole indiqué n'est pas actif, l'hôte de destination peut envoyer un message Destination injoignable à l'hôte de source.

Un autre cas est celui où un datagramme doit être fragmenté pour pouvoir être transmis par un routeur alors que le fanion Ne pas fragmenter est établi. Dans ce cas, le routeur doit éliminer le datagramme et peut retourner un message Destination injoignable.

Les codes 0, 1, 4, et 5 peuvent être reçus d'un routeur. Les codes 2 et 3 peuvent être reçus d'un hôte.

4. Message Durée de vie écoulée



Champs IP :

Adresse de destination : réseau et adresse de source des données du datagramme original.

Champs ICMP :

Type : 11

Code : 0 = durée de vie écoulée dans le transit ;

1 = temps de réassemblage de fragment dépassé.

Somme de contrôle : complément à un sur 16 bits de la somme des compléments à un du message ICMP en commençant par le Type ICMP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être zéro. Cette somme de contrôle pourra être remplacée à l'avenir.

En-tête Internet + 64 bits de datagramme de données : L'en-tête Internet plus les 64 premiers bits des données du datagramme original. Ces données sont utilisées par l'hôte pour confronter le message au processus approprié. Si un protocole de niveau supérieur utilise des numéros d'accès, ils sont supposés être dans les 64 premiers bits des données du datagramme original.

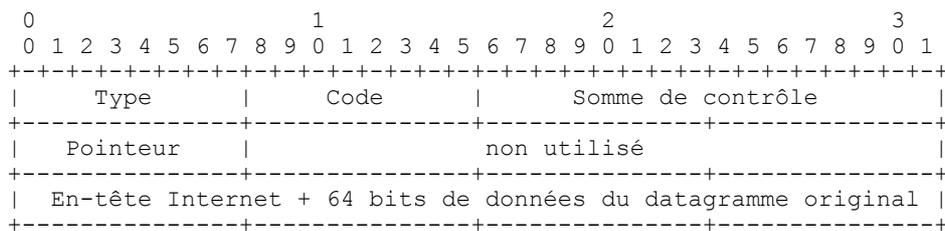
Description

Si un routeur qui traite un datagramme trouve que le champ Durée de vie est à zéro, il doit éliminer le datagramme. Le routeur peut aussi le notifier à l'hôte de source via le message Durée de vie écoulée.

Si un hôte réassemblant un datagramme fragmenté ne peut terminer ce réassemblage à cause de fragments manquants au bout de la temporisation de réassemblage, il doit détruire le datagramme, et peut envoyer un message Durée de vie écoulée.

Si parmi les fragments reçu, aucun ne porte le numéro 0, il n'est pas utile d'envoyer ce message.

Le code 0 peut être reçu d'un routeur. Un code 1 peut être reçu d'un hôte.

5. Message Problème de paramètre**Champs IP :**

Adresse de destination : réseau et adresse de source des données du datagramme original.

Champs ICMP :

Type : 12

Code : 0 = l'erreur est indiquée par le pointeur.

Somme de contrôle : complément à un sur 16 bits de la somme des compléments à un du message ICMP en commençant par le Type ICMP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être zéro. Cette somme de contrôle pourra être remplacée à l'avenir.

Pointeur : Si code = 0, identifie l'octet où l'erreur a été détectée.

En-tête Internet + 64 bits de datagramme de données : L'en-tête Internet plus les 64 premiers bits des données du datagramme original. Ces données sont utilisées par l'hôte pour confronter le message au processus approprié. Si un protocole de niveau supérieur utilise des numéros d'accès, ils sont supposés être dans les 64 premiers bits des données du datagramme original.

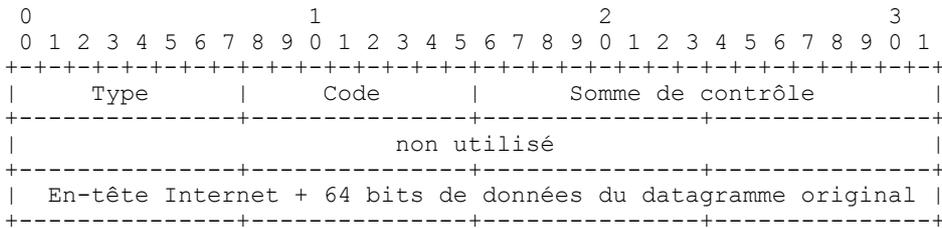
Description

Si le routeur où l'hôte traitant le datagramme rencontre un problème avec des paramètres d'en-tête l'empêchant de finir son traitement, le datagramme doit être détruit. Une source potentielle de ce problème est la présence d'arguments invalides dans une option. Le routeur ou l'hôte peut aussi en avertir la source via le message Problème de paramètre. Ce message n'est envoyé que si l'erreur a été causée par le datagramme à éliminer.

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 des options sont présentes) 20 indique une erreur sur le code de type de la première option.

Un code 0 peut être reçu d'un routeur ou d'un hôte.

6. Message Extinction de source



Champs IP :

Adresse de destination : réseau et adresse de source des données du datagramme original.

Champs ICMP :

Type : 4

Code : 0

Somme de contrôle : complément à un sur 16 bits de la somme des compléments à un du message ICMP en commençant par le Type ICMP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être zéro. Cette somme de contrôle pourra être remplacée à l'avenir.

En-tête Internet + 64 bits de datagramme de données : L'en-tête Internet plus les 64 premiers bits des données du datagramme original. Ces données sont utilisées par l'hôte pour confronter le message au processus approprié. Si un protocole de niveau supérieur utilise des numéros d'accès, ils sont supposés être dans les 64 premiers bits des données du datagramme original.

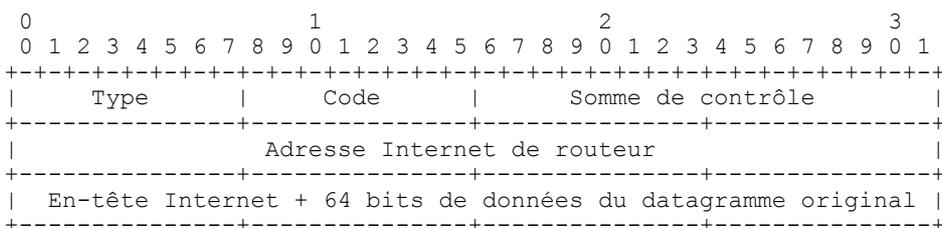
Description

Un routeur peut éliminer des datagrammes Internet si il manque d'espace de mémoire pour mettre en file d'attente les datagrammes à émettre sur le prochain réseau sur le chemin du réseau de destination. Si un routeur élimine un datagramme, un hôte de destination peut aussi envoyer un message Extinction de source à l'hôte Internet de source du datagramme. Un hôte de destination peut aussi envoyer un message Extinction de source si les datagrammes arrivent trop rapidement pour qu'ils puissent être traités. Le message Extinction de source est une demande à l'hôte de source de diminuer le débit d'émission de données vers la destination Internet. Le routeur peut envoyer un message Extinction de source pour chaque message qu'il élimine. À réception d'un message Extinction de source, l'hôte de source devrait réduire son débit d'émission porrs la destination spécifiée jusqu'à ce qu'il ne reçoive plus de messages Extinction de source du routeur. L'hôte de source peut alors graduellement augmenter son débit de sortie jusqu'à de qu'il reçoive de nouveau des messages Extinction de source.

Le routeur ou hôte peut envoyer le message Extinction de source quand il approche de sa limite de capacité plutôt que d'attendre que la capacité soit dépassée. Ceci veut dire que le datagramme de données qui a déclenché l'émission du message Extinction de source peut être livré.

Le code 0 peut être reçu d'un hôte ou d'un routeur.

7. Message Redirection



Champs IP :

Adresse de destination : réseau et adresse de source des données du datagramme original.

Champs ICMP :

Type : 5

Code : 0 = Redirection de datagramme pour le réseau.

1 = Redirection de datagramme pour l'hôte.

2 = Redirection de datagramme pour le type de service et le réseau.

3 = Redirection de datagramme pour le type de service et l'hôte.

Somme de contrôle : complément à un sur 16 bits de la somme des compléments à un du message ICMP en commençant par le Type ICMP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être zéro. Cette somme de contrôle pourra être remplacée à l'avenir.

Adresse Internet de routeur : Adresse du routeur auquel le trafic à destination du réseau spécifié dans le champ Réseau de destination Internet des données du datagramme original devrait être envoyé.

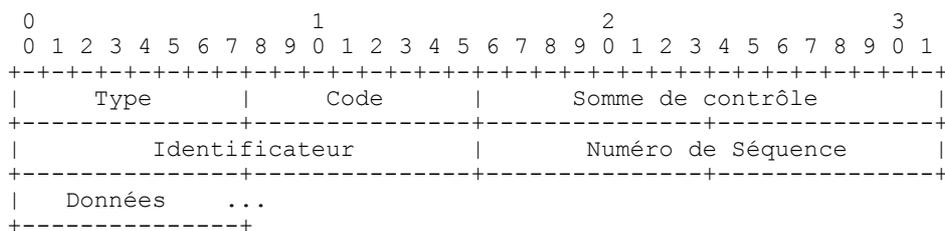
En-tête Internet + 64 bits de datagramme de données : L'en-tête Internet plus les 64 premiers bits des données du datagramme original. Ces données sont utilisées par l'hôte pour confronter le message au processus approprié. Si un protocole de niveau supérieur utilise des numéros d'accès, ils sont supposés être dans les 64 premiers bits des données du datagramme original.

Description

Un routeur peut envoyer un message Redirection à un hôte dans la situation suivante. Un routeur, G1, reçoit un datagramme Internet en provenance d'un hôte situé un réseau sur lequel se trouve le routeur. Le routeur, G1, vérifie ses tableaux d'acheminement et obtient l'adresse du routeur suivant, G2, situé sur le chemin du réseau de destination Internet du datagramme, X. Si G2 et l'hôte identifié par l'adresse Internet de source du datagramme se trouvent sur le même réseau, un message Redirection est envoyé à l'hôte de source. Le message Redirection conseille à la source d'envoyer son trafic pour le réseau X directement au routeur G2, car c'est un chemin plus court pour la destination. Le routeur transmet les données du datagramme original à leur destination Internet.

Pour les datagrammes avec des options Acheminement de source IP et l'adresse du routeur dans le champ Adresse de destination, aucun message Redirection n'est envoyé même si il existe un meilleur chemin vers la destination finale que celui l'adresse suivante dans le chemin de source.

Les codes 0, 1, 2, et 3 peuvent être reçus d'un routeur.

8. Message Écho et Réponse d'écho**Champs IP :**

Adresses : L'adresse de la source dans un message d'écho va être la destination du message Réponse d'écho. Pour former un message Réponse d'écho, il suffit d'inverser les adresses de source et de destination, et de changer le code de type à 0, puis de recalculer la somme de contrôle.

Champs ICMP :

Type : 8 = message Écho;

0 = message Réponse d'écho.

Code : 0

Somme de contrôle : complément à un sur 16 bits de la somme des compléments à un du message ICMP en commençant par le Type ICMP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être zéro. Si la longueur totale est impaire, les données reçues sont bourrées avec un octet de zéros pour calculer la somme de contrôle. Cette somme de contrôle pourra être remplacée à l'avenir.

Identifiant : Si le code = 0, un identifiant permettant d'associer l'écho et la réponse d'écho, peut être zéro.

Numéro de séquence : Si le code = 0, un numéro de séquence permet d'associer l'écho et sa réponse, peut être zéro.

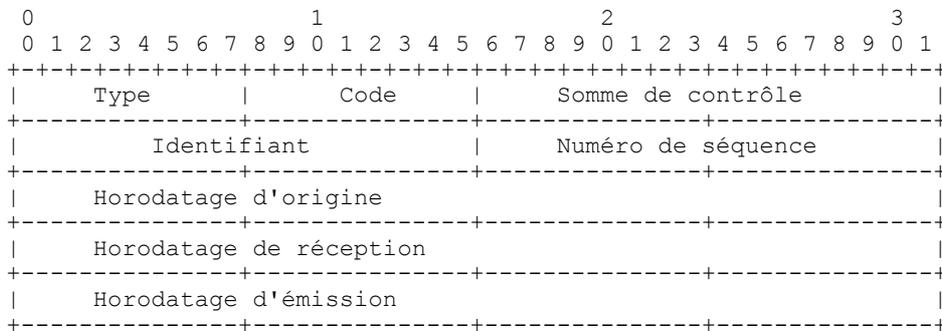
Description

Les données reçues dans un message Écho doivent être retournées dans le message Réponse d'écho.

L'identifiant et le numéro de séquence peuvent être utilisés par l'expéditeur du message Écho pour aider à associer les réponses aux demandes d'écho. Par exemple, l'identifiant pourrait être utilisé comme l'est un accès pour TCP ou UDP pour identifier une session, et le numéro de séquence pourrait être incrémenté pour chaque demande d'écho envoyée. Celui qui fait écho retournera les mêmes valeurs dans la réponse d'écho.

Le code 0 peut être reçu d'un routeur ou d'un hôte.

9. Message Horodatage ou Réponse d'horodatage



Champs IP :

Adresses : L'adresse de la source dans un message Horodatage va être la destination du message Réponse d'horodatage. Pour former un message Réponse d'horodatage, on intervertit simplement l'adresse de source et l'adresse de destination, on change le code de type à la valeur 14, et la somme de contrôle est recalculée.

Champs ICMP :

Type : 13 pour le message Horodatage ;
14 pour le message Réponse d'horodatage.

Code : 0

Somme de contrôle : complément à un sur 16 bits de la somme des compléments à un du message ICMP en commençant par le Type ICMP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être zéro. Cette somme de contrôle pourra être remplacée à l'avenir.

Identifiant : Si code = 0, un identifiant pour aider à associer l'horodatage et sa réponse, peut être zéro.

Numéro de séquence : Si code = 0, un numéro de séquence pour aider à associer l'horodatage et sa réponse, peut être zéro.

Description

Les données reçues (un horodatage) dans le message sont retournées dans la réponse, additionnées d'un horodatage supplémentaire. L'horodatage est de 32 bits des millisecondes depuis minuit GMT. Une utilisation de ces horodatages est décrite par Mills [RFC0778].

L'horodatage d'origine est l'heure à laquelle l'expéditeur a modifié pour la dernière fois le message avant de l'envoyer, l'horodatage de réception donne l'heure à laquelle celui qui fait écho l'a touché à réception, et l'horodatage d'émission est l'heure à laquelle celui qui fait écho a touché le message pour la dernière fois en l'envoyant.

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 insérée dans l'horodatage pourvu que le bit de poids fort de l'horodatage soit établi (à 1) pour indiquer cette valeur non standard.

L'identifiant et le numéro de séquence peuvent être utilisés par l'émetteur de l'horodatage pour aider à associer les réponses et les demandes. Par exemple, l'identifiant pourrait être utilisé comme l'est un accès pour TCP ou UDP pour identifier une session, et le numéro de séquence pourrait être incrémenté à chaque demande envoyée. La destination retournera ces mêmes valeurs dans la réponse.

Le code 0 peut être reçu d'un routeur ou d'un hôte.

10. Message Demande d'Informations ou Réponse d'informations

0																1																2																3															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9																								
Type									Code									Somme de contrôle																																													
Identifiant																Numéro de séquence																																															

Champs IP :

Adresses : L'adresse de la source dans un message Demande d'informations va être la destination du message Réponse d'informations. Pour former un message Réponse d'informations, l'adresse de source et l'adresse de destination son simplement inversées, le code de type est changé à la valeur 16, et la somme de contrôle est recalculée.

Champs ICMP :

Type : 15 pour le message Demande d'informations ;
16 pour le message Réponse d'informations.

Code : 0

Somme de contrôle : complément à un sur 16 bits de la somme des compléments à un du message ICMP en commençant par le Type ICMP. Pour calculer la somme de contrôle, le champ Somme de contrôle devrait être zéro. Cette somme de contrôle pourra être remplacée à l'avenir.

Identifiant : Si code = 0, un identifiant pour aider à associer la demande et sa réponse, peut être zéro.

Numéro de séquence : Si code = 0, un numéro de séquence pour aider à associer la demande et sa réponse, peut être zéro.

Description

Ce message peut être envoyé avec le réseau de source dans le champ Source de l'en-tête IP et des champs Adresse de destination à 0 (ce qui signifie "ce" réseau). Le module IP qui répond devrait envoyer la réponse avec des adresses entièrement renseignées. Par ce message, un hôte peut demander à un routeur le numéro du réseau sur lequel il est situé.

L'identifiant et le numéro de séquence peuvent être utilisés par l'envoyeur de l'écho pour aider à faire correspondre les réponses et les demandes. Par exemple, l'identifiant pourrait être utilisé comme l'est un accès dans TCP ou UDP, pour identifier une session, et le numéro de séquence pourrait être incrémenté pour chaque de demande envoyée. La destination retourne les mêmes valeurs dans la réponse.

Le code 0 peut être reçu d'un routeur ou d'un hôte.

11. Résumé des types de Message

- 0 Réponse d'écho
- 3 Destination injoignable
- 4 Extinction de source
- 5 Redirection
- 8 Écho
- 11 Durée de vie écoulée
- 12 Problème de paramètre

- 13 Horodatage
- 14 Réponse d'horodatage
- 15 Demande d'informations
- 16 Réponse d'informations

12. Références

- [IEN48] Cerf, V., "The Catenet Model for Internetworking," IEN 48, Information Processing Techniques Office, Defense Advanced Research Projects Agency, juillet 1978.
- [IEN30] Strazisar, V., "Gateway Routing: An Implementation Specification", IEN 30, Bolt Beranek and Newman, avril 1979.
- [IEN109] Strazisar, V., "How to Build a Gateway", IEN 109, Bolt Beranek and Newman, août 1979.
- [RFC0778] D. Mills, "Le service d'horloge Internet DCNET", avril 1981. (*Historique*)
- [RFC0791] J. Postel, éd., "Protocole Internet - Spécification du [protocole du programme Internet](#)", STD 5, septembre 1981.