Groupe de travail Réseau
Request for Comments : 4443
RFC rendue obsolète : 2463
RFC mise à jour : 2780
Catégorie : En cours de normalisation

A. Conta, Transwitch
S. Deering, Cisco Systems
M. Gupta, éd., Tropos Networks
mars 2006
Traduction Claude Brière de L'Isle

Spécification du protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)

Statut du présent mémoire
Le présent document spécifie un protocole de normalisation Internet pour la communauté Internet, et appelle à discussion et suggestions en vue de son amélioration. Prière de se rapporter à l'édition en cours des "Internet Official Protocol Standards" (normes officielles du protocole Internet) (STD 1) pour connaître l'état de la normalisation et le statut du présent protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit le format d'un ensemble de messages de contrôle utilisés dans le protocole de message de contrôle Internet pour le protocole Internet version 6 (IPv6) (ICMPv6, *Internet Control Message Protocol*). ICMPv6 est le protocole de message de contrôle Internet pour le protocole Internet version 6 (IPv6).

Table des matières

1. Introduction

Le protocole Internet version 6 (IPv6) utilise le protocole de message de contrôle Internet (ICMP) comme défini pour IPv4 [RFC0792], avec un certain nombre de changements. Le protocole résultant est appelé ICMPv6 et a une valeur de Prochain en-tête IPv6 de 58.

Le présent document décrit le format d'un ensemble de messages de contrôle utilisés dans ICMPv6. Il ne décrit pas les procédures pour utiliser ces messages pour réaliser des fonctions comme celle de découverte de la MTU de chemin ; ces procédures sont décrites dans d'autres documents (par exemple, [RFC1981]). D'autres documents peuvent aussi introduire des types supplémentaires de message ICMPv6, tels que les messages de découverte de voisin [RFC2461], soumis aux règles générales pour les messages ICMPv6 données à la Section 2 du présent document.

La terminologie définie dans la spécification IPv6 [RFC2460] et dans la spécification de l'acheminement et l'adressage IPv6 [RFC3513] s'applique aussi au présent document.

Le présent document rend obsolète la [RFC2463] et met à jour la [RFC2780].

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans ce document sont à interpréter comme décrit dans la [RFC2119].

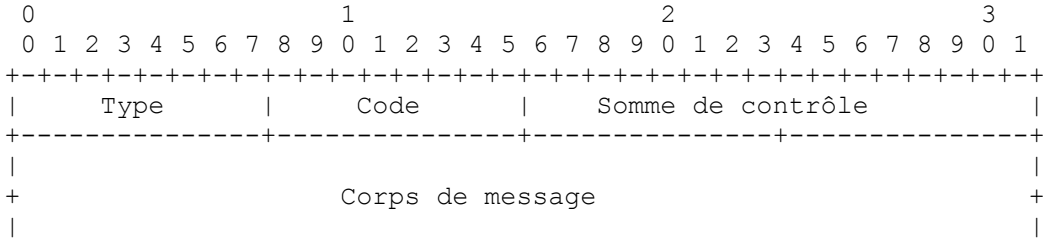
2. ICMPv6 (ICMP pour IPv6)

ICMPv6 est utilisé par les nœuds IPv6 pour faire rapport des erreurs rencontrées dans le traitement des paquets, et pour effectuer d'autres fonctions de couche Internet telles que les diagnostics ("ping" ICMPv6). ICMPv6 fait partie intégrante de IPv6, et le protocole de base (tous les messages et comportements exigés par la présente spécification) DOIT être pleinement mis en œuvre par tout nœud IPv6.

2.1 Format général de message

Tout message ICMPv6 est précédé d'un en-tête IPv6 et de zéro, un ou plusieurs en-têtes d'extension IPv6. L'en-tête ICMPv6 est identifié par une valeur Prochain en-tête de 58 dans l'en-tête immédiatement précédant. (Ceci est différent de la valeur utilisée pour identifier ICMP pour IPv4.)

Les messages ICMPv6 ont le format général suivant :



Le champ Type indique le type du message. Sa valeur détermine le format des données restantes.

Le champ Code dépend du type du message. Il est utilisé pour créer un niveau supplémentaire de granularité de type de message.

Le champ Somme de contrôle est utilisé pour détecter une corruption des données dans le message ICMPv6 et les parties de l'en-tête IPv6.
Les messages ICMPv6 sont groupés en deux classes : les messages d'erreur et les messages d'information. Les messages d'erreur sont identifiés comme tels par un zéro au bit de plus fort poids de leur valeur du champ Type de message. Donc, les messages d'erreur ont des types de message de 0 à 127 ; les messages d'information ont des types de message de 128 à 255.

Le présent document définit les formats de message pour les messages ICMPv6 suivants :
Messages d'erreur ICMPv6 :

1	Destination injoignable	(voir au paragraphe 3.1)
2	Paquet trop gros	(voir au paragraphe 3.2)
3	Durée dépassée	(voir au paragraphe 3.3)
4	Problème de paramètre	(voir au paragraphe 3.4)
100	Expérimentation privée	
101	Expérimentation privée	
127	Réservé pour l'expansion des messages d'erreur ICMPv6	

Messages d'information ICMPv6 :

128	Demande d'écho	(voir au paragraphe 4.1)
129	Réponse d'écho	(voir au paragraphe 4.2)
200	Expérimentation privée	
201	Expérimentation privée	
255	Réservé pour l'expansion des messages d'information ICMPv6.	

Les valeurs de Type 100, 101, 200, et 201 sont réservées pour les expérimentations privées. Elles ne sont pas destinées à une utilisation générale. On s'attend à ce que plusieurs expériences concurrentes soient faites avec les mêmes valeurs de type. Toute utilisation à grande échelle et/ou incontrôlée devrait obtenir des allocations réelles, comme défini à la Section 6.

Les valeurs de Type 127 et 255 sont réservées pour une future expansion de la gamme de valeur de type si il en était besoin à l'avenir. Les détails en sont laissés à des travaux futurs. Une façon possible de le faire qui ne causerait aucun problème avec les mises en œuvre actuelles est que si le type est égal à 127 ou 255, le champ de code devrait être utilisé pour la nouvelle allocation. Les mises en œuvre existantes vont ignorer les nouvelles allocations comme spécifié au paragraphe 2.4, (b). Les nouveaux messages qui utilisent ces valeurs de type étendues pourraient allouer des champs dans le corps de message pour ses valeurs de code.

Les Sections 3 et 4 décrivent les formats de message pour les messages d'erreur ICMPv6 des types 1 à 4 et les types de message d'information 128 et 129.

L'inclusion d'au moins le début du paquet invocateur est destiné à permettre à l'origine d'un paquet qui a résulté en un message d'erreur ICMPv6 d'identifier le protocole et le processus de couche supérieure qui ont envoyé le paquet.

2.2 Détermination de l'adresse de source du message

Un nœud qui génère un message ICMPv6 doit déterminer les adresses à la fois de source et de destination IPv6 dans l'en-tête IPv6 avant de calculer la somme de contrôle. Si le nœud a plus d'une adresse d'envoi individuel, il DOIT choisir l'adresse de source du message comme suit :

(a) Si le message est une réponse à un message envoyé à une des adresses d'envoi individuel du nœud, l'adresse de source de la réponse DOIT être la même adresse.

(b) Si le message est une réponse à un message envoyé à toute autre adresse, telle que
- une adresse de groupe de diffusion groupée,
- une adresse d'envoi à la cantonade mise en œuvre par le nœud, ou
- une adresse d'envoi individuel qui n'appartient pas au nœud,

l'adresse de source du paquet ICMPv6 DOIT être une adresse d'envoi individuel appartenant au nœud. L'adresse DEVRAIT être choisie conformément aux règles qui seraient utilisées pour choisir l'adresse de source pour tout autre paquet généré par le nœud, en fonction de l'adresse de destination du paquet. Cependant, elle PEUT être choisie d'une autre façon si cela conduit à un choix plus informé d'une adresse accessible à partir de la destination du paquet ICMPv6.

2.3 Calcul de la somme de contrôle du message

La somme de contrôle est le complément à un sur 16 bits de la somme des compléments à un du message ICMPv6 entier, commençant par le champ Type du message ICMPv6, et précèdé d'un "pseudo en-tête" de champs d'en-tête IPv6, comme spécifié au paragraphe 8.1 de la [RFC2460]. La valeur de Prochain en-tête utilisée dans le pseudo en-tête est 58. (L'inclusion d'un pseudo en-tête dans la somme de contrôle ICMPv6 est un changement par rapport à IPv4 ; voir la [RFC2460] pour la raison de ce changement.)

Pour calculer la somme de contrôle, le champ Somme de contrôle est d'abord mis à zéro.

2.4 Règles de traitement du message

Les mises en œuvre DOIVENT observer les règles suivantes lors du traitement des messages ICMPv6 (d'après la [RFC1122]) :

(a) Si un message d'erreur ICMPv6 d'un type inconnu est reçu à sa destination, il DOIT être passé au processus de couche supérieure générateur du paquet qui a causé l'erreur, lorsque il peut être identifié (voir au paragraphe 2.4, (d)).

(b) Si un message d'information ICMPv6 de type inconnu est reçu, il DOIT être éliminé en silence.

(c) Tout message d'erreur ICMPv6 (type < 128) DOIT inclure autant du paquet (invoquant) IPv6 en cause (le paquet qui a causé l'erreur) que possible sans faire que le paquet du message d'erreur excède la MTU IPv6 minimum [RFC2460].

(d) Dans les cas où le protocole de couche Internet est obligé de passer un message d'erreur ICMPv6 au processus de couche supérieure, le type du protocole de couche supérieure est extrait du paquet original (contenu dans le corps du message d'erreur ICMPv6) et utilisé pour choisir le processus de couche supérieure approprié pour traiter l'erreur.

Dans les cas où il n'est pas possible de restituer le type de protocole de couche supérieure d'après le message ICMPv6, le message ICMPv6 est abandonné en silence après tout traitement de couche IPv6. Un exemple de ce cas est celui d'un message ICMPv6 avec une quantité inhabituellement grande d'en-têtes d'extension qui n'ont pas le type de protocole de couche supérieure à cause de la troncature du paquet original pour satisfaire à la limite de MTU minimum IPv6 [RFC2460]. Un autre exemple est celui d'un message ICMPv6 avec un en-tête d'extension ESP pour lequel il n'est pas possible de déchiffrer le paquet original à cause d'une troncature ou de l'indisponibilité de l'état nécessaire pour déchiffrer le paquet.

(e) Un message d'erreur ICMPv6 NE DOIT PAS être généré par suite de la réception de ce qui suit :
(e.1) un message d'erreur ICMPv6,
(e.2) un message redirection ICMPv6 [RFC2461],
(e.3) un paquet destiné à une adresse IPv6 de diffusion groupée. (Il y a deux exceptions à cette règle : (1) le message Paquet trop gros (paragraphe 3.2) pour permettre le fonctionnement de la découverte de la MTU du chemin pour la diffusion groupée IPv6, et (2) le message Problème de paramètre, code 2 (paragraphe 3.4) rapportant une option IPv6 non reconnue (voir au paragraphe 4.2 de la [RFC2460]) qui a les deux bits de poids fort du type d'option réglés à 10),
(e.4) un paquet envoyé comme diffusion groupée de couche de liaison (les exceptions de e.3 s'appliquent à ce cas),
(e.5) un paquet envoyé comme diffusion de couche de liaison (les exceptions de e.3 s'appliquent à ce cas),
(e.6) un paquet dont l'adresse de source n'identifie pas de façon univoque un seul nœud -- par exemple, l'adresse IPv6 inspécifiée, une adresse IPv6 de diffusion groupée, ou une adresse connue par l'origine du message ICMP comme étant une adresse IPv6 d'envoi à la cantonade.

(f) Finalement, afin de limiter les coûts en bande passante et transmission causés par la génération de messages d'erreur ICMPv6, un nœud IPv6 DOIT limiter le taux de messages d'erreur ICMPv6 qu'il génère. Cette situation peut survenir lorsque une source qui envoie un flux de paquets erronés échoue à prendre en compte les messages d'erreur ICMPv6 résultants.

La limitation du taux de transmission des messages ICMP sort du domaine d'application de la présente spécification.

Une méthode recommandée pour mettre en œuvre la fonction de limitation du taux est un baquet de jetons qui limite le taux moyen de transmission à N, où N peut être des paquets/s ou une fraction de la bande passante de la liaison rattachée, mais permettant jusqu'à B messages d'erreur transmis dans une salve, tant que la moyenne à long terme n'est pas dépassée.

Les mécanismes de limitation de taux qui ne peuvent pas prendre en compte le trafic sporadique (par exemple, traceroute) ne sont pas recommandés ; par exemple, la mise en œuvre d'un simple temporisateur, permettant un message d'erreur toutes les T millisecondes (avec même de faibles valeurs pour T) n'est pas raisonnable.

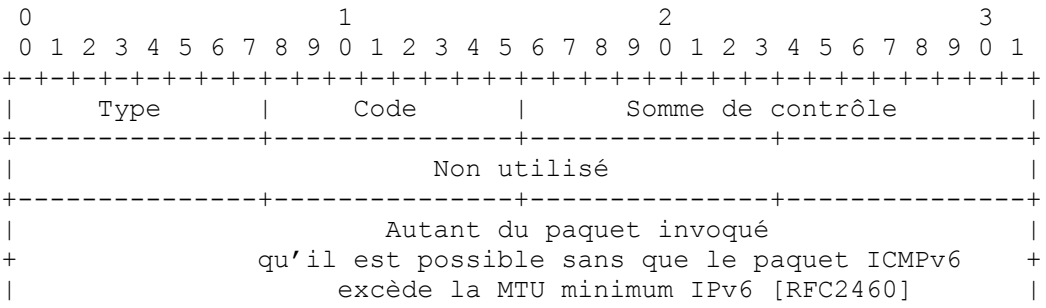
Les paramètres de limitation de taux DEVRAIENT être configurables. Dans le cas de mise en œuvre d'un baquet de jetons, les meilleurs paramètres par défaut dépendent d'où il est prévu de déployer la mise en œuvre (par exemple, sur un routeur en plein champ ou dans un hôte incorporé). Par exemple, dans un appareil de taille petite/moyenne, les valeurs par défaut possibles pourraient être B = 10, N = 10/s.

Note : les restrictions sous (e) et (f) ci-dessus prennent le pas sur toute exigence formulée ailleurs dans ce document pour la génération de messages d'erreur ICMP.

Les paragraphes qui suivent décrivent les formats pour les messages ICMPv6 ci-dessus.

3. Messages d'erreur ICMPv6

3.1 Message Destination injoignable



Champs IPv6 :

Adresse de destination / Copié du champ Adresse de source du paquet invoquant.

Champs ICMPv6 :
Type : 1
Code : 0 – Pas de chemin pour la destination
1 – Communication interdite administrativement avec la destination
2 – Au delà de la portée de l'adresse de source
3 – Adresse injoignable
4 – Accès injoignable
5 – Adresse de source refusée par la politique d'entrée/sortie
6 – Rejet du chemin vers la destination
Non utilisé : Ce champ est non utilisé pour toutes les valeurs de code. Il doit être initialisé à zéro par l'origine et ignoré par le receveur.

Description
Un message Destination injoignable DEVRAIT être généré par un routeur, ou par la couche IPv6 du nœud d'origine, en réponse à un paquet qui ne peut pas être livré à son adresse de destination pour des raisons autres que l'encombrement. (Un message ICMPv6 NE DOIT PAS être généré si un paquet est abandonné à cause de l'encombrement.)

Si la raison de l'échec de la livraison est l'absence d'une entrée qui corresponde dans le tableau d'acheminement du nœud de transmission, le champ Code est réglé à 0.

(Cette erreur ne peut survenir que dans des nœuds qui ne contiennent pas de "chemin par défaut" dans leurs tableaux d'acheminement.)

Si la raison de l'échec de livraison est l'interdiction administrative (par exemple, un "filtre pare-feu") le champ Code est réglé à 1.

Si la raison de l'échec de livraison est que la destination est au delà de la portée de l'adresse de source, le champ Code est réglé à 2. Cette condition ne peut survenir que lorsque la portée de l'adresse de source est plus petite que la portée de l'adresse de destination (par exemple, lorsque un paquet a une adresse de source de liaison locale et une adresse de destination de porté mondiale) et le paquet ne peut pas être livré à la destination sans quitter la portée de l'adresse de source.

Si la raison de l'échec de livraison ne peut pas être transposé en un des autres codes, le champ Code est réglé à 3. Un exemple de tels cas est l'incapacité à résoudre l'adresse de destination IPv6 en une adresse de liaison correspondante, ou un problème spécifique de la liaison.

Un cas spécifique dans lequel un message Destination injoignable est envoyé avec un code 3 est en réponse à un paquet reçu par un routeur d'une liaison point à point, destiné à une adresse au sein d'un sous-réseau alloué à la même liaison (autre qu'une de celles des propres adresses du routeur receveur). Dans un tel cas, le paquet NE DOIT PAS être retransmis sur la liaison d'arrivée.

Un nœud de destination DEVRAIT générer un message Destination injoignable avec le code 4 en réponse à un paquet pour lequel le protocole de transport (par exemple, UDP) n'a pas d'écoutant, si ce protocole de transport n'a pas de moyens de

remplacement pour informer l'envoyeur.

Si la raison de l'échec de livraison est que le paquet avec cette adresse de source n'est pas permis à cause des politiques de filtrage d'entrée ou de sortie, le champ Code est réglé à 5.

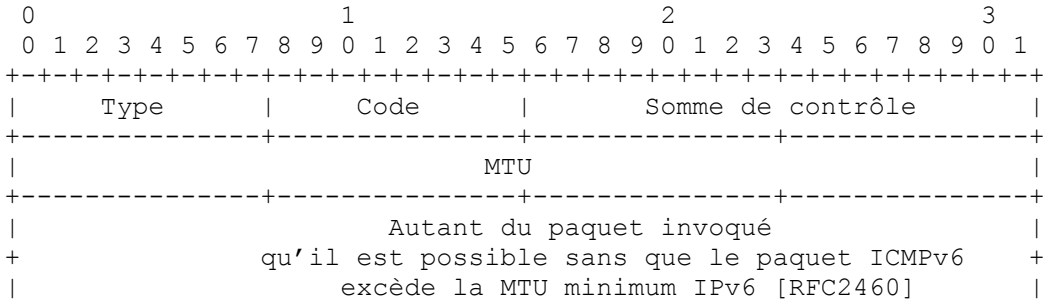
Si la raison de l'échec de livraison est que le chemin vers la destination est un chemin rejeté, le champ Code est réglé à 6. Cela peut survenir si le routeur a été configuré pour rejeter tout le trafic pour un certain préfixe

Les codes 5 et 6 sont des sous-ensembles plus informatifs du code 1.

Pour des raisons de sécurité, il est recommandé que les mises en œuvre permettent que l'envoi de messages ICMP Destination injoignable soit désactivé, de préférence interface par interface.

Notification de couche supérieure
Un nœud qui reçoit le message ICMPv6 Destination injoignable DOIT le notifier au processus de couche supérieure si ce processus peut être identifié (voir au paragraphe 2.4, (d)).

3.2 Message Paquet trop gros



Champs IPv6 :

Adresse de destination / Copiée du champ Adresse de source du paquet invoquant.

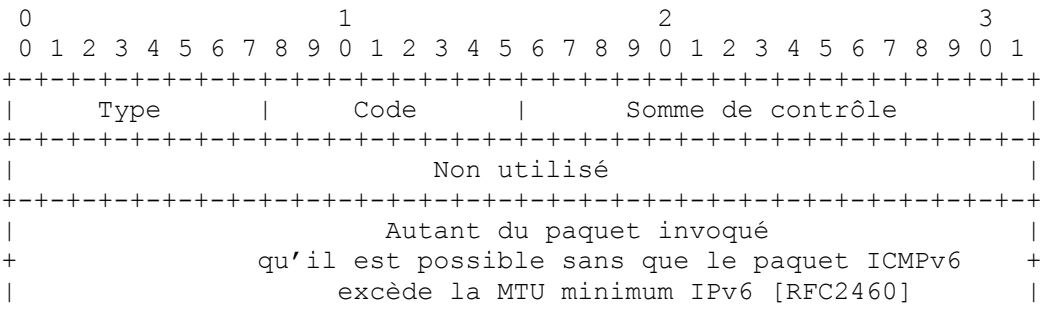
Champs ICMPv6 :
Type : 2
Code : Réglé à 0 (zéro) par l'origine et ignoré par le receveur.
MTU : Unité de transmission maximum de la liaison de prochain bond.

Description
Un message Paquet trop gros DOIT être envoyé par un routeur en réponse à un paquet qu'il ne peut pas transmettre parce que le paquet est plus gros que la MTU de la liaison sortante. Les informations qui sont dans ce message sont utilisées au titre du processus de découverte de la MTU de chemin [RFC1981].

Générer un message Paquet trop gros fait exception à une des règles sur le moment où générer un message d'erreur ICMPv6. À la différence des autres messages, il est envoyé en réponse à un paquet reçu avec une adresse IPv6 de destination de diffusion groupée, ou avec une adresse de diffusion groupée de couche de liaison ou de diffusion de couche de liaison.

Notification de couche supérieure
Un message Paquet trop gros entrant DOIT être passé au processus de couche supérieure si le processus pertinent peut être identifié (voir au paragraphe 2.4, (d)).

3.3 Message Durée dépassée



Champs IPv6 :

Adresse de destination / Copiée du champ Adresse de source du paquet invoquant.

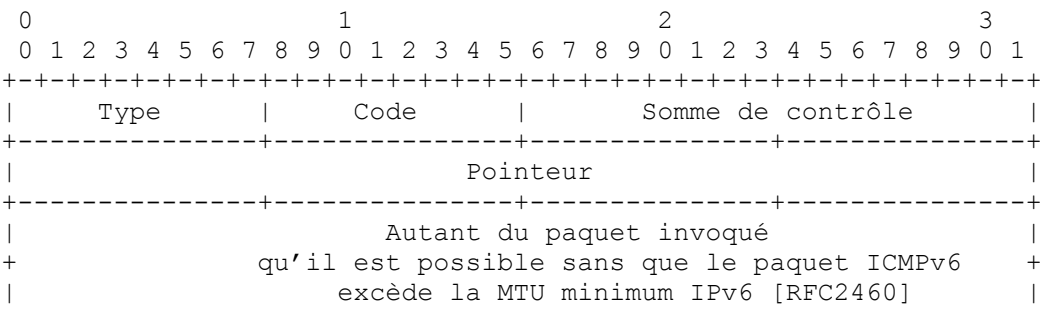
Champs ICMPv6 :
Type : 3
Code : 0 – Limite de bonds excédée dans un transit
1 – Délai de réassemblage de fragment excédé
Non utilisé : Ce champ est inutilisé pour toutes les valeurs de code. Il doit être initialisé à zéro par l'origine et ignoré à réception.

Description
Si un routeur reçoit un paquet avec une limite de bonds de zéro, ou si un routeur décrémente la limite de bonds d'un paquet à zéro, il DOIT éliminer le paquet et générer un message ICMPv6 Durée dépassée avec le code 0 à la source du paquet. Cela indique soit une boucle d'acheminement, soit une valeur de limite de bonds initiale trop petite.

Un message ICMPv6 Durée dépassée avec le code 1 est utilisé pour rapporter une fin de temporisation de réassemblage de fragment, comme spécifié au paragraphe 4.5 de la [RFC2460].

Notification de couche supérieure
Un message entrant Durée dépassée DOIT être passé au processus de couche supérieure si le processus pertinent peut être identifié (voir au paragraphe 2.4, (d)).

3.4 Message Problème de paramètre



Champs IPv6 :

Adresse de destination : Copiée du champ Adresse de source du paquet invoquant.

Champs ICMPv6 :
Type : 4
Code : 0 – Un champ d'en-tête erroné a été rencontré
1 – Un type de prochain en-tête non reconnu a été rencontré
2 – Une option IPv6 non reconnue a été rencontrée
Pointeur : Identifie le décalage d'octet au sein du paquet invoquant où l'erreur a été détectée. Le pointeur va pointer au delà de la fin du paquet ICMPv6 si le champ erroné est au delà de ce qui peut tenir dans la taille maximum d'un message d'erreur ICMPv6.

Description
Si un nœud IPv6 qui traite un paquet trouve un problème avec un champ de l'en-tête IPv6 ou des en-têtes d'extension, tel qu'il ne puisse terminer le traitement du paquet, il DOIT éliminer le paquet et DEVRAIT générer un message ICMPv6 Problème de paramètre à la source du paquet, indiquant le type et la localisation du problème.

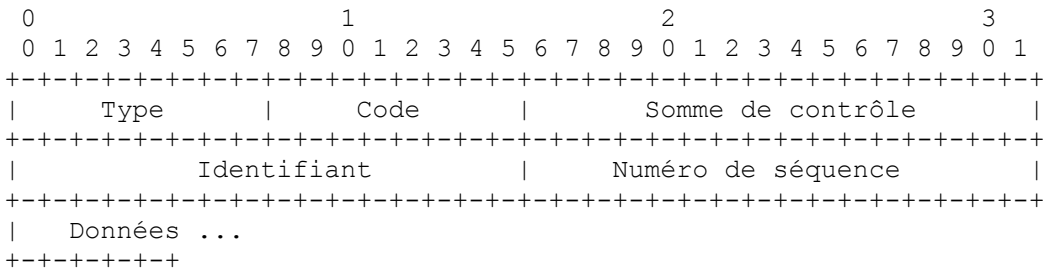
Les codes 1 et 2 sont des sous-ensembles plus informatifs du code 0.

Le pointeur identifie l'octet de l'en-tête du paquet d'origine où l'erreur a été détectée. Par exemple, un message ICMPv6 avec un champ Type de 4, un champ Code de 1, et un champ Pointeur de 40 indiquera que l'en-tête d'extension IPv6 qui suit l'en-tête IPv6 du paquet d'origine contient une valeur non reconnue de champ Prochain en-tête.

Notification de couche supérieure
Un nœud qui reçoit ce message ICMPv6 DOIT le notifier au processus de couche supérieure si le processus pertinent peut être identifié (voir au paragraphe 2.4, (d)).

4. Messages d'information ICMPv6

4.1 Message Demande d'écho



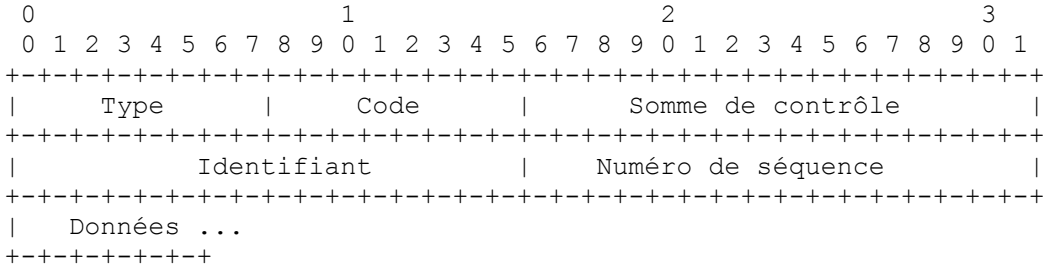
Champs IPv6 :
Adresse de destination : Toute adresse IPv6 légale

Champs ICMPv6 :
Type : 128
Code : 0
Identifiant : Identifiant pour aider à faire correspondre les réponses d'écho à cette demande d'écho. Peut être zéro.
Numéro de séquence : Numéro de séquence pour aider à faire correspondre les réponses d'écho à cette demande d'écho. Peut être zéro.
Données : Zéro, un, ou plusieurs octets de données arbitraires.

Description
Chaque nœud DOIT mettre en œuvre une fonction de répondeur d'écho ICMPv6 qui reçoit les demandes d'écho et génère les réponses d'écho correspondantes. Un nœud DEVRAIT aussi mettre en œuvre une interface de couche application pour générer les demandes d'écho et recevoir les réponses d'écho, pour les besoins de diagnostic.

Notification de couche supérieure
Les messages Demande d'écho PEUVENT être passés aux processus qui reçoivent les messages ICMP.

4.2 Message Réponse d'écho



Champs IPv6 :

Adresse de destination : Copiée du champ Adresse de source du paquet Demande d'écho invoquant.

Champs ICMPv6 :

Type :	129
Code :	0
Identifiant :	L'identifiant du message Demande d'écho invoquant.
Numéro de séquence :	Numéro de séquence du message Demande d'écho invoquant.
Données :	Les données du message Demande d'écho invoquant.

Description
Chaque nœud DOIT mettre en œuvre une fonction de répondeur d'écho ICMPv6 qui reçoit les demandes d'écho et génère les réponses d'écho correspondantes. Un nœud DEVRAIT aussi mettre en œuvre une interface de couche application pour générer les demandes d'écho et recevoir les réponses d'écho, pour des besoins de diagnostic.

L'adresse de source d'une réponse d'écho envoyée en réponse à un message Demande d'écho en envoi individuel DOIT être la même que l'adresse de destination de ce message Demande d'écho.

Une réponse d'écho DEVRAIT être envoyée en réponse à un message Demande d'écho envoyé à une adresse IPv6 en diffusion groupée ou en envoi individuel. Dans ce cas, l'adresse de source de la réponse DOIT être une adresse d'envoi individuel appartenant à l'interface sur laquelle le message Demande d'écho a été reçu.

Les données reçues dans le message ICMPv6 Demande d'écho DOIVENT être retournées entièrement et non modifiées dans le messages Réponse d'écho ICMPv6.

Notification de couche supérieure
Les messages Réponse d'écho DOIVENT être passés au processus qui a généré un message Demande d'écho. Un message Réponse d'écho PEUT être passé à des processus qui n'ont pas généré le message Demande d'écho.

Noter qu'il n'y a pas de limitation à la quantité de données qui peuvent être mises dans les messages Demande d'écho et Réponse d'écho.

5. Considérations pour la sécurité

5.1 Authentification et confidentialité des messages ICMP

Les échanges de paquet du protocole ICMP peuvent être authentifiés en utilisant l'en-tête Authentification IP de la [RFC4301] ou l'en-tête Encapsulation de charge utile de sécurité IP de la [RFC4302]. La confidentialité pour les échanges de paquet de protocole ICMP peut être réalisée en utilisant l'en-tête Encapsulation de charge utile de sécurité IP de la [RFC4302].

La [RFC4303] décrit en détails le traitement IPsec du trafic ICMP.

5.2 Attaques ICMP

Les messages ICMP peuvent faire l'objet de diverses attaques. Un exposé complet se trouve dans l'architecture de sécurité IP de la [RFC2401]. Voici un bref exposé sur ces attaques et leur prévention :

1. Les messages ICMP peuvent faire l'objet d'actions destinées à faire croire au receveur que le message est venu d'une source différente de celle qui a généré le message. La protection contre cette attaque peut être réalisée en appliquant le mécanisme d'authentification IPv6 de la [RFC4301] au message ICMP.

2. Les messages ICMP peuvent faire l'objet d'actions destinées à faire que le message ou sa réponse aille à une destination différente de celle où le générateur du message avait l'intention de l'envoyer. La protection contre cette attaque peut être réalisée en utilisant l'en-tête Authentification de la [RFC4301] ou l'en-tête Encapsulation de charge utile de sécurité de la [RFC4302]. L'en-tête Authentification assure la protection contre le changement de l'adresse de source et de destination du paquet IP. L'en-tête Encapsulation de charge utile de sécurité ne fournit pas cette protection, mais le

calcul de somme de contrôle ICMP comporte les adresses de source et de destination, et l'en-tête Encapsulation de charge utile de sécurité protège la somme de contrôle. Donc, la combinaison de la somme de contrôle et de l'en-tête Encapsulation de charge utile de sécurité assure la protection contre cette attaque. La protection fournie par l'en-tête Encapsulation de charge utile de sécurité ne sera pas aussi forte que celle fournie par l'en-tête d'authentification.

3. Les messages ICMP peuvent faire l'objet de changements dans les champs du message, ou dans la charge utile. L'authentification [RFC4301] ou le chiffrement [RFC4302] du message ICMP protège contre de telles actions.

4. Les messages ICMP peuvent être utilisés pour tenter des attaques de déni de service en renvoyant des paquets IP erronés. Une mise en œuvre qui suit correctement le paragraphe 2.4, (f) de la présente spécification sera protégée par le mécanisme de limitation du taux d'erreurs ICMP

5. L'exception numéro 2 à la règle e.3 du paragraphe 2.4 donne à un nœud malveillant l'opportunité de causer une attaque de déni de service à une source de diffusion groupée. Un nœud malveillant peut envoyer un paquet en diffusion groupée avec une option destination inconnue marquée comme obligatoire, avec l'adresse de source IPv6 d'une source en envoi individuel valide. Un grand nombre de nœuds de destination vont envoyer un message ICMP Problème de paramètre à la source de diffusion groupée, causant une attaque de déni de service. La façon dont le trafic de diffusion groupée est transmis par les routeurs de diffusion groupée exige que le nœud malveillant fasse partie du chemin de diffusion groupée correct, c'est-à-dire, près de la source de la diffusion groupée. Cette attaque ne peut être évitée que par la sécurisation du trafic en diffusion groupée. La source de diffusion groupée devrait faire attention lorsqu elle envoie du trafic en diffusion groupée avec les options de destination marquées comme obligatoires, parce qu'elles peuvent causer une attaque de déni de service contre elle-même si l'option de destination est inconnue d'un grand nombre de destinations.

6. Comme les messages ICMP sont passés aux processus de couche supérieure, il est possible d'effectuer des attaques sur les protocoles de couche supérieure (par exemple, TCP) avec ICMP [RFC5927]. Il est recommandé que les couches supérieures effectuent une forme de validation des messages ICMP (en utilisant les informations contenues dans la charge utile du message ICMP) avant d'agir sur eux. Les vérifications d'une validation réelle sont spécifiques des couches supérieure et sortent du domaine d'application de la présente spécification. La protection de la couche supérieure avec IPsec atténue ces attaques.

Les messages d'erreur ICMP signalent des conditions d'erreur réseau qui ont été rencontrées lors du traitement d'un datagramme Internet. Selon le scénario concerné, les conditions d'erreur rapportées peuvent n'être pas solubles à court terme. Donc, la réaction aux messages d'erreur ICMP peut dépendre non seulement du type et du code d'erreur mais aussi d'autres facteurs, tels que l'heure à laquelle les messages d'erreur sont reçus, de la connaissance préalable des conditions d'erreur du réseau qui ont été rapportées, et de la connaissance du scénario de réseau dans lequel fonctionne l'hôte receveur.

6. Considérations relatives à l'IANA

6.1 Procédure pour l'allocation de nouvelles valeurs de type et de code ICMPv6

L'en-tête ICMP IPv6 défini dans le présent document contient les champs suivants qui portent les valeurs allouées à partir de l'espace de noms géré par l'IANA : Type et code. Les valeurs du champ Code sont définies par rapport à une valeur de type spécifique.

Les valeurs pour les champs Type ICMP IPv6 sont allouées en utilisant la procédure suivante :

1. L'IANA devrait allouer et enregistrer de façon permanente les nouveaux codes de type ICMPv6 à partir des publications de RFC de l'IETF. Ceci pour tous les types de RFC, incluant celles en cours de normalisation, pour information, et expérimentales, dont l'origine est l'IETF et dont la publication a été approuvée par l'IESG.

2. Les groupes de travail de l'IETF avec consensus du groupe de travail et l'approbation du directeur de zone peuvent demander des allocations de code de type ICMPV6 disponibles à l'IANA. L'IANA marquera les valeurs comme "réclamables à l'avenir".

   Le marquage "réclamable à l'avenir" sera retiré lorsque sera publiée une RFC documentant le protocole comme défini en 1. Cela rendra l'allocation permanente et mettra la référence à jour sur le site IANA de la Toile.

   Au moment où 85 % des valeurs de type ICMPv6 auront été allouées, l'IETF reprendra les allocations marquées "réclamables à l'avenir" et informera l'IANA de celles qui devraient être réclamées et réallouées.

3. Les demandes d'allocation de nouvelles valeurs de type ICMPv6 de l'extérieur de l'IETF ne peuvent être faites qu'à travers la publication d'un document de l'IETF, selon le 1 ci-dessus. Noter aussi que les documents publiés comme "contributions de l'éditeur des RFC" [RFC3978] ne sont pas considérées comme des documents de l'IETF.

L'allocation de nouvelles valeurs de code pour les valeurs de type définies dans le présent document exigent une action de normalisation ou l'approbation de l'IESG. La politique d'allocation des valeurs de code pour les nouveaux types ICMP IPv6 non définis dans le présent document devrait être définie dans le document qui définit les nouvelles valeurs de type.

6.2 Allocations pour ce document

La mise à jour des allocations se trouve à : http://www.iana.org/assignments/icmpv6-parameters

L'IANA a réalloué le type ICMPv6 1 "Destination injoignable" code 2, qui n'était pas alloué dans la [RFC2463] à :
2 – Au delà de la portée de l'adresse de source

L'IANA a alloué les deux nouvelles valeurs de code suivantes au type ICMPv6 1 "Destination injoignable" :
5 – Adresse de source refusée par la politique d'entrée/sortie
6 – Rejet du chemin vers la destination

L'IANA a alloué les valeurs de nouveau type suivantes :
100 – Expérimentation privée
101 – Expérimentation privée
127 – Réservé pour l'expansion des messages d'erreur ICMPv6
200 – Expérimentation privée
201 – Expérimentation privée
255 – Réservé pour l'expansion des messages d'information ICMPv6

7. Références

7.1 Références normatives

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981. *(MàJ par la* RFC6633)

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, octobre 1989. *(MàJ par la* RFC6633)

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par 5095,6564 ; D.S)*

[RFC2461] T. Narten, E. Nordmark, W. Simpson, "Découverte de voisins pour IP version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4861) *(D.S.)*

[RFC2463] A. Conta, S. Deering, "Protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4443) *(D.S.)*

[RFC3978] S. Bradner, éd., "Droits de l'IETF dans les contributions", mars 2005. (*Obsolète, voir* RFC5378). (*MàJ par* RFC4748)

7.2 Références pour information

[RFC1981] J. McCann, S. Deering, J. Mogul, "Découverte de la MTU de chemin pour IP version 6", août 1996. *(D.S.)*

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2780] S. Bradner et V. Paxson, "Lignes directrices pour les allocations par l'IANA des valeurs du protocole Internet et des en-têtes qui s'y rapportent", BCP 37, mars 2000.

[RFC3513] R. Hinden et S. Deering, "Architecture d'adressage du protocole Internet version 6 (IPv6)", avril 2003. (*Obsolète, voir* RFC4291)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401*)*

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC5927] F. Gont, "Attaques ICMP contre TCP", juillet 2010. *(Information)*

8. Remerciements

Le présent document est dérivé des documents ICMP précédents des groupes de travail SIPP et IPng.

Le groupe de travail IPng et en particulier Robert Elz, Jim Bound, Bill Simpson, Thomas Narten, Charlie Lynn, Bill Fink, Scott Bradner, Dimitri Haskin, Bob Hinden, Jun-ichiro Itojun Hagino, Tatuya Jinmei, Brian Zill, Pekka Savola, Fred Templin, et Elwyn Davies (dans l'ordre chronologique) ont fourni des informations et des retours importants pour la révision de ce document.

Bob Hinden était l'éditeur du document.

Appendice A - Changements depuis la RFC2463

Les changements suivants ont été apportés à la RFC2463:

- Réécriture du résumé pour le rendre un petit peu plus élaboré.
- Correction de fautes de frappe au paragraphe 2.4, où la référence au point e.2 désignait en fait le point e.3.
- Retrait des méthodes fondée sur le temporisateur et fondée sur la bande passante de l'exemple du mécanisme de limitation du taux de message d'erreur ICMP. Ajout de la méthode fondée sur la baquet de jetons.
- Ajout de la spécification que tous les messages d'erreur ICMP devront avoir exactement 32 bits de données spécifiques du type, afin que les receveurs puissent trouver de façon fiable le paquet invoquant incorporé même lorsque ils ne reconnaissent pas le type de message ICMP.
- Dans la description des messages Destination injoignable, Code 3, ajout de la règle prohibant la retransmission de paquets sur des liaisons point à point sur lesquelles il ont été reçus, si leurs adresses de destination appartiennent à la liaison elle même ("règle anti ping-pong").
- Ajout de la description du code 1 Durée dépassée (fin de temporisation de réassemblage de fragment).
- Ajout des messages "Au delà de la portée de l'adresse de source", "Adresse de source refusée par la politique d'entrée/sortie", et "Rejet du chemin vers la destination" à la famille des messages d'erreur ICMP de type "Destination injoignable" (paragraphe 3.1).
- Réservation de certaines valeurs de type ICMP pour l'expérimentation.
- Ajout d'une note au paragraphe 2.4 qui spécifie les règles de préséance du traitement du message ICMP.
- Ajout de la Redirection ICMP à la liste du paragraphe 2.4, (e) des cas dans lesquels les messages d'erreur ICMP ne sont pas à générer.
- Changements rédactionnels mineurs au paragraphe 2.3 sur le calcul de la somme de contrôle, et au paragraphe 5.2.
- Précision au paragraphe 4.2, concernant le message Réponse d'écho, que l'adresse de source d'une réponse d'écho à une demande d'écho en envoi à la cantonade devrait être une adresse d'envoi individuel, comme dans le cas de la diffusion groupée.
- Révision de la section Considérations pour la sécurité. Ajout de l'utilisation de l'en-tête Encapsulation de charge utile de sécurité pour l'authentification. Changement de l'exigence d'une option "d'interdiction de messages ICMP non authentifiés" de DEVRAIT à PEUT.
- Ajout d'une nouvelle attaque dans la liste des attaques ICMP possibles au paragraphe 5.2.
- Séparation des références en normatives et pour information.
- Ajout d'une référence à la RFC 2780 et ajout d'une note disant que ce document met à jour la RFC2780.
- Ajout d'une procédure pour l'allocation de nouvelles valeurs de type et code ICMPv6 dans la section de considérations

relatives à l'IANA.

- Remplacement du mot "envoie" par "génère" pour rendre clair que les paquets ICMP sont transmis hors de la portée de cette spécification.
- Changement des références aux documents ESP et AH à jour.
- Ajout des références au document à jour d'architecture de sécurité IPsec.
- Ajout d'une exigence DEVRAIT pour permettre de désactiver l'envoi de messages ICMP Destination injoignable.
- Simplification du choix de l'adresse de source du paquet ICMPv6.
- Réorganisation du format général de message (paragraphe 2.1).
- Retrait du format général de message du paragraphe 2.1. Il se réfère maintenant aux Sections 3 et 4 pour les formats de paquet.
- Ajout de texte sur les attaques des protocoles de transport qui pourraient être causées par ICMP.

Adresse des auteurs

Alex Conta
Transwitch Corporation
3 Enterprise Drive
Shelton, CT 06484
USA
mél : aconta@txc.com

Stephen Deering
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Mukesh Gupta, Ed.
Tropos Networks
555 Del Rey Avenue
Sunnyvale, CA 94085
téléphone : +1 408-331-6889
mél : mukesh.gupta@tropos.com

Déclaration de droits de reproduction

Propriété intellectuelle

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif (IASA) de l'IETF.