Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 7279
BCP 189
Catégorie : Bonnes pratiques actuelles
ISSN : 2070-1721

M. Shore, No Mountain Software
C. Pignataro, Cisco Systems, Inc.

mai 2014
Traduction Claude Brière de L'Isle

Politique d'utilisation acceptable pour les nouveaux types et codes ICMP

Résumé
Dans le présent document on donne une description de base du rôle de ICMP dans la pile IP et des directives pour son utilisation future.

Le motif du présent document réside dans les soucis découlant du manque de clarté concernant le moment où il convient d'ajouter de nouveaux types et/ou codes du protocole de message de commande Internet (ICMP, *Internet Control Message Protocol*). Ces soucis ont mis en lumière le besoin de décrire les politiques sur quand il est souhaitable d'ajouter de nouvelles caractéristiques à ICMP et quand cela ne l'est pas.

Table des Matières

1. Introduction

Certains soucis ont été récemment exprimés concernant le manque de clarté sur le moment où devraient être ajoutés de nouveaux types et codes de message à ICMP (incluant ICMPv4 [RFC0792] et ICMPv6 [RFC4443]). On propose une politique

concernant le moment de placer (ou ne pas placer une nouvelle fonctionnalité dans ICMP.

Le présent document est le résultat de discussions entre les experts ICMP au sein du groupe d'intérêt technique Diagnostics IP [DIAGN] de la zone Opérations et gestion (OPS, *Operations and Management*) et les soucis exprimés par la direction de la zone OPS.

Noter que le présent document ne remplace pas les "Lignes directrices pour les allocations par l'IANA des valeurs du protocole Internet et des en-têtes qui s'y rapportent" [RFC2780], qui spécifie les bonnes pratiques et processus pour l'allocation de valeurs dans les registres de l'IANA mais ne décrit pas les politiques à appliquer dans le processus de normalisation.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Politique d'utilisation acceptable

Dans le présent document, on décrit une politique d'utilisation acceptable pour les nouveaux types et codes de message ICMP, et on donne quelques indications de fond sur la politique.

En résumé, tous les futurs types de message ajoutés à ICMP devraient se limiter à deux grandes catégories :

1. pour informer le générateur d'un datagramme qu'une anomalie du plan de transmission a été rencontrée en aval. Le générateur du datagramme doit être capable de déterminer si le datagramme a été ou non éliminé en examinant le message ICMP.

2. pour découvrir et porter des informations dynamiques sur un nœud (autres que les informations généralement portées dans les protocoles d'acheminement) pour découvrir et porter des paramètres spécifiques du réseau, et pour découvrir les routeurs et hôtes en ligne.

Normalement, ICMP NE DEVRAIT PAS être utilisé pour mettre en œuvre un protocole d'acheminement ou de gestion de réseau de caractère général. Cependant, ICMP n'a pas de rôle à jouer en matière de transport d'informations dynamiques sur un réseau, ce qui relèverait de la catégorie 2 ci-dessus.

2.1 Classification des types de message existants

Ce paragraphe fait le point des types de message existants selon la taxonomie décrit à la Section 2 au moment de la publication.

Rapport d'anomalie du plan de transmission IPv4 :
3 : Destination injoignable
4 : Affaiblissement de source (déconseillé)
6 : Adresse d'hôte de remplacement (déconseillé)
11 : Durée dépassée
12 : Problème de paramètre
31 : Erreur de conversion de datagramme (déconseillé)

Découverte de routeur ou hôte IPv4 :
0 : Réponse d'écho
5 : Redirection
8 : Écho
9 : Annonce de routeur
10 : Sollicitation de routeur
13 : Horodatage
14 : Réponse d'horodatage
15 : Demande d'information (déconseillé)
16 : Réponse d'information (déconseillé)
17 : Demande de gabarit d'adresse (déconseillé)
18 : Réponse de gabarit d'adresse (déconseillé)
30 : Traceroute (déconseillé)
32 : Redirection d'hôte mobile (déconseillé)

33 : IPv6 Où-es-tu? (déconseillé)
34 : IPv6 Je-suis-là (déconseillé)
35 : Demande d'enregistrement mobile (déconseillé)
36 : Réponse d'enregistrement mobile (déconseillé)
37 : Demande de nom de domaine (déconseillé)
38 : Réponse de nom de domaine (déconseillé)
39 : SKIP (déconseillé)
40 : Photuris
41 : Messages ICMP utilisé par des protocoles de mobilité expérimentaux comme Seamoby

Noter que certains types de message ICMP ont été formellement déconseillés par la [RFC6918].

Rapport d'anomalie du plan de transmission IPv6 :
1 : Destination injoignable
2 : Paquet trop gros
3 : Temps dépassé
4 : Problème de paramètre
150 : messages ICMP utilisé par des protocoles de mobilité expérimentaux comme Seamoby

Découvert de routeur ou hôte IPv6 :
128 : Demande d'écho
129 : Réponse d'écho
130 : Interrogation d'écoutant de diffusion groupée
131 : Rapport d'écoutant de diffusion groupée
132 : Écoutant de diffusion groupée terminé
133 : Sollicitation de routeur
134 : Annonce de routeur
135 : Sollicitation de voisin
136 : Annonce de voisin
137 : Message de redirection
138 : Dénumérotation de routeur
139 : Interrogation d'informations de nœud ICMP
140 : Réponse d'informations de nœud ICMP
141 : Message de sollicitation de découverte inverse de voisin
142 : Message d'annonce de découverte inverse de voisin
143 : Rapport d'écoutant de diffusion groupée version 2
144 : Message de demande de découverte d'adresse d'agent de rattachement
145 : Message de réponse de découverte d'adresse d'agent de rattachement
146 : Sollicitation de préfixe mobile
147 : Annonce de préfixe mobile
148 : Message de sollicitation de chemin de certification
149 : Message d'annonce de chemin de certification
150 : Messages ICMP utilisés par des protocole de mobilité expérimentaux comme Seamoby
151 : Annonce de routeur de diffusion groupée
152 : Sollicitation de routeur de diffusion groupée
153 : Terminaison de routeur de diffusion groupée
154 : Messages FMIPv6
155 : Message de commande RPL

2.1.1 Utilisation d'ICMP comme protocole d'acheminement

Comme mentionné à la Section 2, utiliser ICMP comme protocole d'acheminement ou de gestion de réseau d'objet général n'est pas conseillé et NE DEVRAIT PAS être utilisé de cette façon.

ICMP a un rôle dans l'Internet comme partie intégrante de la couche IP ; ce n'est pas un protocole d'acheminement ni un protocole de transport pour les autres couches, y compris les informations d'acheminement. D'un point de vue plus pragmatique, certaines des caractéristiques clés de ICMP en font un choix discutable comme protocole d'acheminement. Ces caractéristiques clés incluent que ICMP est fréquemment filtré, n'est pas authentifié, et facilement maquillé. De plus, le traitement de matériel spécialiste de ICMP va déranger le déploiement d'un protocole d'acheminement ou de gestion fondé sur ICMP.

2.1.2 Quelques notes sur RPL

RPL, le protocole d'acheminement IPv6 pour les réseaux à faible puissance et à pertes (voie la [RFC6550]) utilise ICMP comme transport. Á cet égard, c'est une exception parmi les types de message ICMP. Noter que, bien que RPL soit un protocole d'acheminement IP, il n'est pas déployé sur l'Internet général ; il est limité à des réseaux spécifiques, contenus.

Cela devrait être considéré comme une anomalie et n'est pas un modèle pour de futurs types de message ICMP. C'est-à-dire que ICMP n'est pas destiné à être un transport pour les autres protocoles et NE DEVRAIT PAS être utilisé de cette façon dans de futures spécifications. En particulier, alors qu'il est adéquat d'utiliser ICMP comme un protocole de découverte, il ne possède pas toutes les capacités de l'acheminement.

2.2 Applications qui utilisent ICMP

Certaines applications utilisent les notifications d'erreur de ICMP, ou même créent délibérément des conditions anormales afin d'obtenir des messages ICMP. Ces messages ICMP sont alors utilisés pour générer des retours à la couche supérieure. Certaines de ces applications incluent des exemples très répandus, comme PING, TRACEROUTE, et la découverte de la MTU de chemin (PMTUD). Ces utilisations sont considérées comme acceptables parce que elles utilisent des types de message ICMP existants et ne changent pas la fonction d'ICMP.

2.3 Extension d'ICMP

Des messages ICMP multiparties sont spécifiés dans la [RFC4884] en définissant un mécanisme d'extension pour des messages ICMP choisis. Ce mécanisme s'adresse à un problème fondamental de l'extensibilité d'ICMP. Un message ICMP multiparties porte toutes les informations que portaient précédemment les messages ICMP, ainsi que des informations supplémentaires que les applications peuvent exiger.

Certaines extensions ICMP couramment définies incluent des extensions ICMP pour la commutation d'étiquettes multi protocoles [RFC4950] et des extensions ICMP pour l'identification d'interface et de prochain bond [RFC5837].

Les extensions à ICMP DEVRAIENT suivre les exigences de la [RFC4884].

2.4 ICMPv4 contre ICMPv6

Parce que ICMPv6 est utilisé pour la découverte de voisin IPv6, les routeurs IPv6 déployés, les passerelles de sécurité à capacité IPv6, et les pare-feu à capacité IPv6 prennent normalement en charge la configuration de la façon dont les types de messages ICMPv6 spécifiques sont traités. Au contraire, les routeurs IPv4 déployés, les passerelles de sécurité à capacité IPv4, et les pare-feu à capacité IPv4 vont vraisemblablement être moins enclins à laisser un administrateur configurer comment les types de messages spécifiques ICMPv4 sont traités. Donc, à présent, les messages ICMPv6 ont généralement plus de chances de voyager de bout en bout que les messages ICMPv4.

3. Rôle d'ICM dans l'Internet

ICMP était à l'origine destiné à être un mécanisme pour les passerelles ou les hôtes de destination pour faire rapport de conditions aux hôtes de source dans ICMPv4 [RFC0792] ; ICMPv6 [RFC4443] a été modélisé d'après lui. ICMP est aussi utilisé pour effectuer des fonctions de couche IP, comme des diagnostics (par exemple, PING).

ICMP est défini comme faisant partie intégrante de IP et doit être mis en œuvre par tout module IP. Ceci est vrai pour ICMPv4 comme partie intégrante de IPv4 (voir l'introduction de la [RFC0792]), et pour ICMPv6 comme partie intégrante de IPv6 (voir la Section 2 de la [RFC4443]). Lorsque ils ont été définis pour la première fois, les messages ICMP étaient vus comme des messages IP qui ne portaient aucune données de couche supérieure. On pouvait se demander si le terme de "contrôle" était utilisé parce que les messages ICMP n'étaient pas des messages de "données".

Le mot "contrôle" dans le nom du protocole ne décrivait pas la fonction de ICMP (c'est-à-dire qu'il ne "contrôle" pas l'Internet) ; il est plutôt utilisé pour communiquer sur les fonctions de contrôle dans l'Internet. Par exemple, même si ICMP inclut un type de message de redirection qui affecte le comportement d'acheminement dans le contexte d'un segment de LAN, il n'était pas et n'est pas utilisé comme protocole d'acheminement générique.

4. Considérations sur la sécurité

Le présent document décrit une politique très générale pour l'ajout de types et codes ICMP. Bien qu'une attention particulière doive être portée aux implications de sécurité de tout nouveau type ou code ICMP particulier, cette recommandation ne présente aucune nouvelle considération de sécurité.

Du point de vue de la sécurité, ICMP joue un rôle dans le protocole Photuris [RFC2521]. Mais plus généralement, ICMP n'est pas un protocole sûr et n'inclut pas de dispositifs à utiliser pour découvrir des paramètres de sécurité de réseau ou pour rapporter sur les anomalies de la sécurité réseau dans le plan de transmission.

De plus, de nouvelles fonctionnalités ICMP (par exemple, extensions ICMP, ou nouveaux types ou codes ICMP) doivent examiner les façon potentielles dont on peut abuser de ICMP (par exemple, capture du DoS IP [CA-1998-01]).

5. Remerciements

Le présent document a été à l'origine proposé par Ron Bonica qui y a fait ensuite des révisions et suggestions substantielles,. Des discussions avec Pascal Thubert ont aidé à clarifier l'histoire de l'utilisation de ICMP par RPL. Nous sommes reconnaissants de leur relecture, retours et commentaires à Ran Atkinson, Tim Chown, Joe Clarke, Adrian Farrel, Ray Hunter, Hilarie Orman, Eric Rosen, JINMEI Tatuya, et Wen Zhang, qui ont abouti à un document très amélioré.

6. Références

6.1 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)

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

[RFC4443] A. Conta et autres, "Spécification du protocole de message de contrôle Internet (ICMPv6) pour la version 6 du protocole Internet (IPv6)", mars 2006. (*Remplace* RFC2463) (*MàJ* RFC2780) (*MàJ par* RFC4884) *(D.S.)*

[RFC4884] R. Bonica et autres, "ICMP étendu pour la prise en charge de messages multiparties", avril 2007. (*MàJ* RFC0792, RFC4443) *(P.S. ; MàJ par* RFC8335)

6.2 Références pour information

[CA-1998-01] CERT, "Smurf IP Denial-of-Service Attacks", CERT Advisory CA-1998-01, janvier 1998, <http://www.cert.org/advisories/CA-1998-01.html >.

[DIAGN] "IP Diagnostics Technical Interest Group", < https://svn.tools.ietf.org/area/ops/trac/wiki/TIG_DIAGNOSTICS >.

[RFC2521] P. Karn, W. Simpson, "Messages d'échec de sécurité ICMP", mars 1999. *(Expérimentale)*

[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.

[RFC4950] R. Bonica et autres, "Extensions à ICMP pour la commutation d'étiquettes multiprotocoles", août 2007. *(P.S.)*

[RFC5837] A. Atlas, R. Bonica, C. Pignataro, N. Shen, JR. Rivers, "Extension à ICMP pour l'identification d'interface et du prochain bond", avril 2010. *(P. S.)*

[RFC6550] T. Winter et autres, "RPL :¨protocole d'acheminement IPv6 pour réseaux à faible énergie et enclins aux pertes", mars 2012. *(P.S.)*

[RFC6918] F. Gont, C. Pignataro, "Certains types de messages ICMPv4 sont formellement déconseillés", avril 2013

(*Remplace* RFC1788) (*MàJ* RFC0792, RFC0950) *(P.S.)*

Adresse des auteurs

Melinda Shore
No Mountain Software
PO Box 16271
Two Rivers, AK 99716
US
téléphone : +1 907 322 9522
mél : melinda.shore@nomountain.net

Carlos Pignataro
Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US
mél : cpignata@cisco.com