Notification des erreurs

(Z:\Polys\Internet RES0\8.ICMP.fm- 30 janvier 2013 15:01)

PLAN

- Introduction
- Généralités sur ICMP
- Les messages d'inaccessibilité
- L'écho - Ping
- La durée excessive - Traceroute
- La fragmentation - MTU
- Conclusion

1. Introduction

Internet Control Message Protocol

ICMP a deux rôles :

- Notification des erreurs lors de la transmission de données (IP, TCP, UDP).
- Messages d'administration (contrôle du réseau).

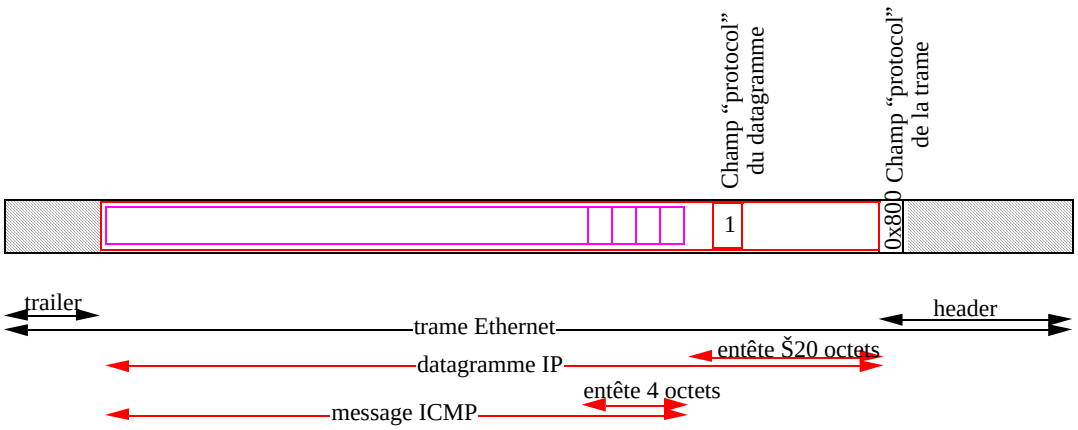
Buts du chapaitre :

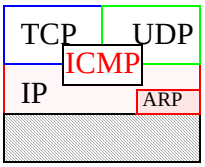
- Découvertes de nouveaux mécanismes
- Rappels sur Internet

C'est un protocole indispensable au bon fonctionnement d'IP.

2. Généralités

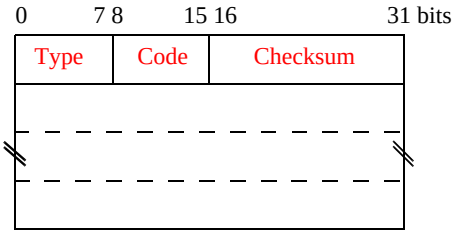
2.1. ICMP et IP et Ethernet





. ICMP gère les événements pour IP, TCP et UDP
. Les messages ICMP sont transportés par des datagrammes IP

2.2. Format général des messages ICMP



Type (8 bits) :
. type du message
. + de 20 types de messages ICMP différents
. 2 grandes catégories :
- message généré à la suite d'une erreur
- message d'administration

Code (8 bits) :
. sous-type du message ICMP

Checksum (16 bits) :
. protège la totalité du message
. procédé de calcul identique à celui de IP, TCP, UDP:
- somme de mots de 16 bits en complément à 1.
. obligatoire

La structure du reste du message dépend du type (1 mot minimum).

2.3. Les types des messages ICMP

Type	Code	Description	Erreur/Administration
0	0	echo reply	A
3		destination unreachable :	
	0	network unreachable	E
	1	host unreachable	E
	2	protocol unreachable	E
	3	port unreachable	E
	4	fragmentation needed and don't seg. bit set	E
	5	source route failed	E
	6	destination network unknown	E
	7	destination host unknown	E
	8	source host isolated	E
	9	destination network administratively prohibited	E
	10	destination host administratively prohibited	E
	11	network unreachable for TOS	E
	12	host unreachable for TOS	E
	13	communication administratively prohibited by filtering	E
	14	host precedence violation	E
	15	precedence cutoff in effect	E
4	0	source quench	E
5		redirect :	
	0	redirect for network	E
	1	redirect for host	E
	2	redirect for TOS and network	E
	3	redirect for TOS and host	E

Les types des messages ICMP (suite)

Type	Code	Description	Erreur/Administration
8	0	echo request	A
9	0	router advertisement	A
10	0	router solicitation	A
11		time to live exceeded :	
	0	during transit	E
	1	during fragment reassembly	E
12		parameter problem:	
	0	bad IP header	E
	1	required option missing	E
13	0	timestamp request	A
14	0	timestamp reply	A
15	0	information request	A
16	0	information reply	A
17	0	address mask request	A
18	0	address mask reply	A
30	0	traceroute	A
31	0	datagram conversion error	A
32	0	mobile station redirection	A
33	0	IPv6 station localisation request	A
34	0	IPv6 station localisation response	A
35	0	mobile station recording request	A
36	0	mobile station recording response	A

3. Inaccessibilité

3.1. Présentation

Lorsqu'un noeud reçoit un datagramme qu'il ne sait pas acheminer !

Message d'erreur émis par les noeuds (routeurs) d'extrémité :

- le noeud ne connaît aucune station ayant l'adresse de destination du datagramme
- le noeud ne gère pas le sous-réseau associé à cette adresse

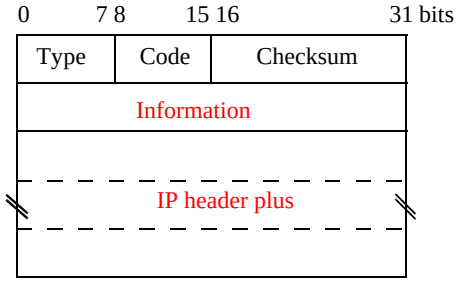
Le message d'erreur est retourné à l'expéditeur. Le champ de données du message d'erreur contient l'entête du datagramme erroné.

Quelques causes :

- l'adresse du datagramme (ou le n° de port du message) a été corrompue
- la station destinatrice a disparue (en panne, éteinte, déplacée, etc.)
- la station destinatrice n'est pas prête à recevoir un tel datagramme :
  - . le message contenu dans le datagramme ne lui convient pas
  - . par exemple : aucun processus n'est affecté au n° port spécifié

    utilisé par le processus de recherche de route : "traceroute"

3.2. Format des messages d'inaccessibilité



ICMP destination unreachable message

Type
- 3 : le destinataire est inaccessible

Code : la cause de l'inaccessibilité :
- hôte ou réseau inaccessible : émis par un routeur ne pouvant retransmettre le datagramme
- port inaccessible : le numéro de port n'a pas de processus affecté (⇒ traceroute)
- fragmentation nécessaire (⇒ MTU discovery)

Information (32 bits) :
- information générale sur le traitement de l'erreur
- champ parfois inutilisé (=0)

IP header :
permet de reconnaître le paquet ayant généré l'erreur.
- l'entête du datagramme IP ayant provoqué la l'erreur.
- inclusivement, les options de l'entête IP.
- plus (au moins) les 8 premiers octets du champ de données du datagramme IP (c'est-à-dire l'entête du protocole de niveau supérieur).

4. Echo

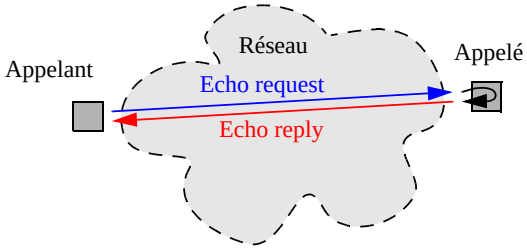
4.1. Principe

Les messages ICMP "Echo" permettent de tester l'accessibilité d'une station.
- attention : les mécanismes de contrôle d'accès peuvent rendre ce test instable (“firewall gateway”)

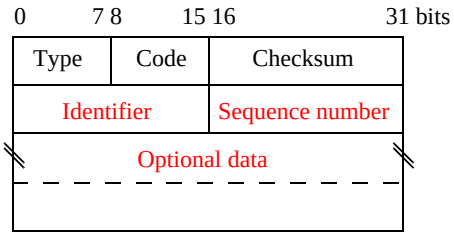
Mesure du temps de propagation aller-retour (RTT : "Round Trip Time")

=> commande *ping*

Exemple : `ping athena`
`athena is alive`
`ping xthena`
`no answer from xthena`
`ping -s -i 10`



4.2. Format des messages d'écho



ICMP echo message

2 types de message d'écho :
- 0 : réponse
- 8 : demande

Code = 0.

Identifier :
- identifie le client (≈ n° de port)
- le PID du processus sous Unix

Sequence number :
- incrémenté à chaque envoi de messages
- "Ping" permet l'envoi périodique (1s)

⇒ Min/Moy/Max/taux d’erreur.

Optional data :
- "Ping" permet l'envoi de messages de taille quelconque.
- les mêmes données à aller et au retour.

⇒ le RTT est composé du délai de propagation et de la durée d'émission.

5. Durée de résidence dépassée

5.1. Principe

Message ICMP généré lorsque le champ TTL d'un datagramme IP arrive à 0,
et que le datagramme est détruit.
Utilisé pour connaître la route entre 2 stations :

- teste l'accessibilité
- la liste des routeurs intermédiaires sur cette route
- la durée de transit entre chaque routeur de cette route

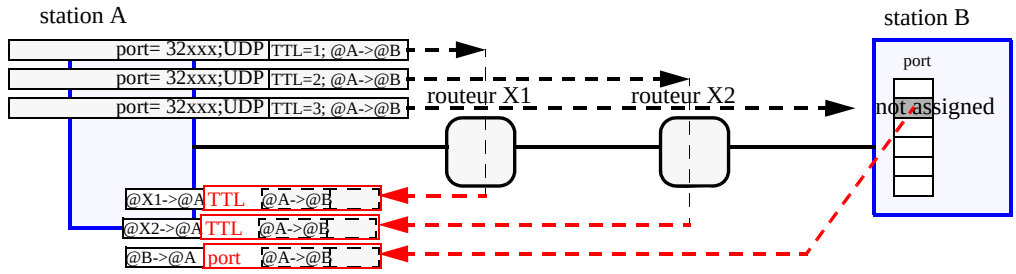
⇒ traceroute

"Traceroute"/"tracert" :

- utilisation conjointe du champ TTL des datagrammes IP
- et des messages ICMP de type “Time exceeded”

5.2. Exemple de fonctionnement de "Traceroute"

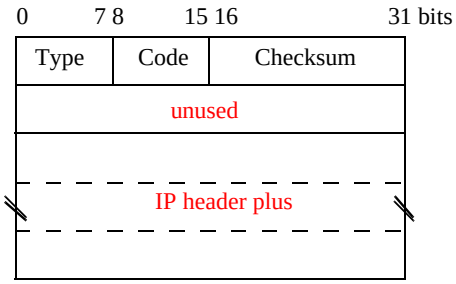
```
A$ traceroute B
```



Exemple de résultat :

- `traceroute to B`
  - `X1 5 ms 4 ms 3 ms`
  - `X2 138 ms _`[2] `ms 141 ms`[1]<--- congestion
  - `B 141 ms 150ms 120`[3] `ms`

5.3. Format des messages de durée excessive



ICMP time exceeded message

Type du message :
- 11 : durée limite de vie du datagramme atteinte.

Code :
- 0 = pendant le transit (aux routeurs).
- 1 = pendant le réassemblage (au récepteur)

Unused :
- champ à zéro

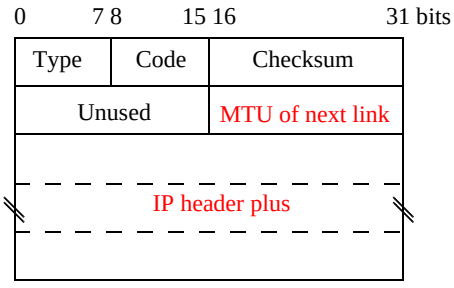
IP header :
- l'entête du datagramme IP ayant provoqué l'erreur.
- inclusivement les options de l'entête IP.
- plus (au moins) les 8 premiers octets du champ de données du datagramme IP.

⇒ au minimum : 28 octets

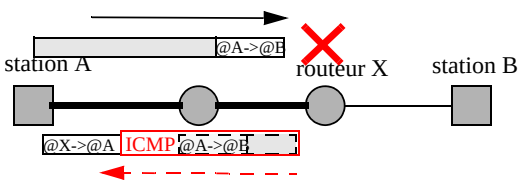
6. Fragmentation

6.1. Format des messages d'erreur de fragmentation

Type, code :
- 3, 4 : erreur lors d'une fragmentation



ICMP fragmentation error message



MTU of next link :
- donne la longueur maximum d'un datagramme pour qu'il puisse franchir la prochaine liaison sans fragmentation.

IP header plus :
- l'entête + options + 8 1er octets du champ data du datagramme IP ayant provoqué cette erreur.

Un message est généré lorsque la fragmentation est nécessaire :
- le MTU de la prochaine liaison est plus petit que la taille du datagramme

mais interdite :
- le datagramme a son bit "do not fragment" positionné.

Le datagramme est détruit par le routeur
Un message ICMP, indiquant que le destinataire est inaccessible à cause de la fragmentation, est émis par le routeur vers l'émetteur.

6.2. La recherche de MTU path

"MTU path discovery"

La fragmentation est coûteuse :
. on peut l'éviter aux routeurs si l'émetteur connaît le MTU path

Cette valeur est variable :
. elle dépend du chemin emprunté
. de la topologie du réseau

=> Procédé de recherche du MTU_P (RFC 1191) :

. on émet les paquets avec le bit "don't fragment" positionné.

. le premier MTU_P choisi est le MTU_L de la source.

. tant qu'on reçoit un message d'erreur de fragmentation, on diminue la taille du paquet (en fonction des longueurs proposées).

. une liste ordonnée de longueurs privilégiées est proposée pour augmenter la vitesse de convergence du processus de recherche.
(min: 68, X25: 508, Ethernet: 1492, 802.5: 2002, FDDI: 4352, 802.4: 8166, TK: 17914, 32000, max: 65535)

Régulièrement chaque station tente d'émettre un paquet avec un MTU_P plus grand (par défaut, toutes les 10 mn, ou 2 mn après avoir augmenté le MTU_P).

7. Conclusion

Le protocole ICMP est indispensable au bon fonctionnement d'Internet :

. informe des cas d'erreur survenant sur IP, TCP et UDP :
- destination inaccessible
- corruption de messages

. permet d'administrer le réseau :
- redirection de route
- annonce de masque d'adressage, de routeurs, etc.
- vérification de l'accessibilité : commandes *traceroute*, *ping*
- gestion de la fragmentation, calcul du "MTU path"
- mise à l'heure (obsolète !)
- aide au contrôle de congestion (inutilisée !)
- station mobile et IPv6 !

Ils existent d'autres fonctions d'administration rendues par d'autres protocoles tout aussi indispensables au fonctionnement d'Internet.