Réseaux

Protocole ICMP

Master Miage 1
Université de Nice - Sophia Antipolis

(second semestre 2009-2010)

Jean-Pierre Lips *(jean-pierre.lips@unice.fr)*
(à partir du cours de Jean-Marie Munier)

Sources bibliographiques

- ✓ Comer (D.E.) : TCP/IP architecture, protocoles, applications - 6ème édition - Dunod 2009/01
- ✓ Comer (D.E.) : Réseaux et Internet - CampusPress 2000
- ✓ Servin (C.) : Réseaux et télécoms - 3ème édition - Dunod 2009
- ✓ Siyan (K.S.) : TCP/IP - 2ème édition - CampusPress 2001

- ✓ RFC 792

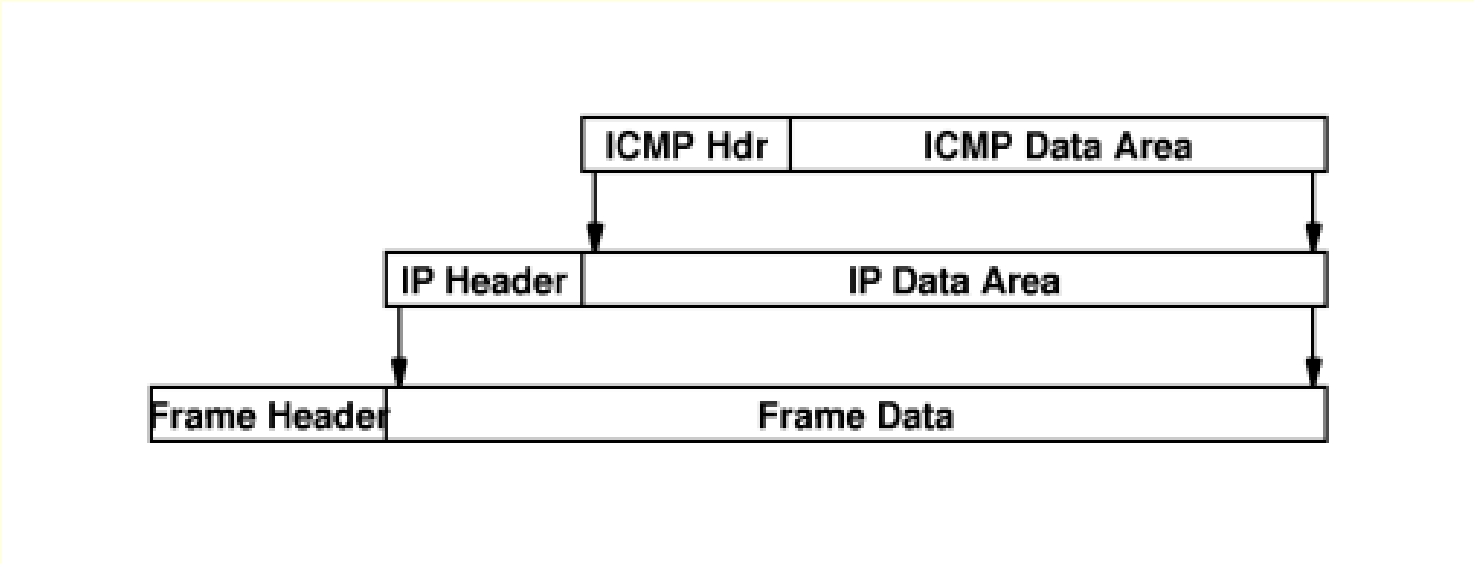
- ✓ Cours UREC du CNRS (www.urec.fr)

Principes

- **ICMP** *(Internet Control Message Protocol)*
- IP et ICMP interdépendants :
  - IP utilise ICMP pour envoyer des messages d'erreur
  - ICMP utilise IP pour transporter ces messages
- ICMP doit être mis en œuvre dans toute implémentation de IP (mais implémentations variées)
- Deux grands types de messages ICMP :
  - messages d'erreur, renvoyés à l'hôte source qui a émis le datagramme IP en erreur
  - messages de supervision
- ICMP signale les conditions d'erreur, sans rendre IP plus fiable

Encapsulation ICMP

- Message ICMP encapsulé dans un datagramme IP (champ **Protocole** de l'en-tête IP = 1)
- Datagramme IP encapsulé dans une trame, pour être transmis



Source : D. E. Comer - Computer Networks and Internets - Prentice Hall 1999

Structure générale

- **Type** (1 octet) : type de service ICMP
- **Code** (1 octet) : subdivision du type de service
- **Total de contrôle** (2 octets) : protection du contenu du message ICMP (même algorithme que IP)
- **Autres champs** (4 octets), selon la valeur du champ Type (numéro de séquence, identificateur, adresse IP…)
- **Données ICMP** :
  - données (Echo), adresse IP, masque d'adresse, date...
  - en-tête IP et 8 premiers octets du datagramme en erreur (messages d'erreur)

Principaux types de messages ICMP

Type	Signification
0	Réponse à une requête d'écho
3	Destination inaccessible
4	Limitation de débit de la source *(Source Quench)*
5	Reroutage *(Redirect)*
8	Requête d'écho
9	Annonce de routeur
10	Sélection de routeur
11	Expiration de délai
12	Problème de paramètre
13	Requête d'horodatage *(Timestamp)*
14	Réponse à une requête d'horodatage
17	Requête de masque d'adresse
18	Réponse à une demande de masque d'adresse

Messages d'écho

- Requête d'écho / Réponse à une requête d'écho
- Permettent de tester l'accessibilité d'un hôte
- Utilitaire **PING** *(Packet INternet Groper)* de fonctionnalités très variées
- Exemple :

```
•  PING www.sears.com: 56 data bytes
64 bytes from searsweb.advantis.com (204.146.164.194): seq=0 time=125. ms
64 bytes from searsweb.advantis.com (204.146.164.194): seq=0 time=123. ms
64 bytes from searsweb.advantis.com (204.146.164.194): seq=0 time=124. ms
64 bytes from searsweb.advantis.com (204.146.164.194): seq=0 time=121. ms
64 bytes from searsweb.advantis.com (204.146.164.194): seq=0 time=122. ms
- - - - www.sears.com PING Statistics - - - -
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 121/122/125
```

Destination inaccessible

- Message ICMP renvoyé par un routeur ou par l'hôte destinataire si un datagramme ne peut pas être remis
- Champ Code permettant de distinguer plusieurs cas.
  Exemples :

Code	**Signification**
0	Réseau inaccessible
1	Hôte inaccessible
2	Protocole inaccessible
3	Port inaccessible
4	Fragmentation nécessaire et flag DF *(Don't Fragment)* activé
5	Echec du routage par la source

Limitation de débit de la source

- Message ICMP ***(Source Quench)*** renvoyé par un routeur en congestion (plus assez de mémoire tampon disponible pour les datagrammes entrants), à l'hôte source du datagramme écarté
- La source doit alors réduire son rythme de transmission
- Pas de moyen explicite pour signaler à la source la fin de l 'état de congestion

Expiration de délai *(Time exceeded)*

- Message envoyé par un routeur lorsque après avoir décrémenté le champ **TTL** d'un datagramme, la durée de vie est nulle et le datagramme est écarté
  - rappel : un routeur décrémente (d'au moins 1) le champ TTL chaque fois qu'il traite un datagramme. Cela évite que, s'il existe des chemins en boucle, du fait de tables de routage erronées, ou modifiées suite à des pannes de liens, un datagramme circule sans fin
- Autre cas : message envoyé par l'hôte de destination dont le temporisateur de réassemblage expire avant réception de tous les fragments d'un datagramme

Autres messages ICMP

- Reroutage *(Redirect)*
  - ✓ message envoyé par un routeur lorsqu'il constate qu'il a reçu un datagramme qui aurait dû arriver sur un autre routeur (le routeur réachemine néanmoins le datagramme). Permet à l'hôte de modifier sa table de routage
- Sélection de routeur / Annonce de routeur
  - ✓ permettent à un hôte de découvrir tous les routeurs existant sur le réseau auquel il est directement connecté
- Problème de paramètre
  - ✓ exemples : valeur invalide du champ Type de Service, paramètres d'une option incorrects...
- Requête / Réponse d'horodatage
  - ✓ requête permettant d'obtenir l'information de date d'un hôte distant, à des fins de synchronisation
- Requête / Réponse de masque d'adresse
  - ✓ requête envoyée par un hôte à un routeur (éventuellement en diffusion) pour obtenir le masque de sous-réseau à utiliser

Trace d'une route

- Utilitaire TRACEROUTE
- Première étape :
  - ✓ envoi d'un message dans un datagramme de durée de vie = 1
  - ✓ décrémentation de TTL et élimination du datagramme par le premier routeur, qui renvoie un **message ICMP d'expiration de délai**
  - ✓ utilisation, par TRACEROUTE, de l'adresse de source de ce message ICMP
- Etapes suivantes : idem, avec TTL=2, 3, 4…
- Le message envoyé par TRACEROUTE est un message UDP vers une application inexistante de l'hôte cible. Lorsque la valeur de TTL permet d'atteindre l'hôte, ce dernier renvoie un **message ICMP de destination inaccessible**.
- Hypothèse : routes relativement stables

Trace d'une route (exemple)

```
traceroute to DANDELION-PATCH.MIT.EDU (18.181.0.31), 40 byte packets
 1 cisco1 (128.10.2.250)  3 ms  2 ms  2 ms
 2 cisco-tel-atm.gw.purdue.edu (128.210.252.22)  2 ms  2 ms  2 ms
 3 h5-0-0.c24-12.Chicago.t3.ans.net (207.24.177.73) 18 ms  18 ms  18 ms
 4 f2-1.t24-0.Chicago.t3.ans.net (140.222.27.221)  20 ms  20 ms  20 ms
 5 h12-1.t40-0.Cleveland.t3.ans.net (140.223.25.30)  32 ms  28 ms  32 ms
 6 h12-1.t36-0.New-York2.t3.ans.net (140.223.37.9)  45 ms  46 ms  46 ms
 7 h1-0.p3233.t3.ans.net (207.25.133.18)  48 ms  46 ms  49 ms
 8 h5-0-0.cambridge1-br1.bbnplanet.net (4.0.1.122)  54 ms  58 ms  55 ms
 9 h3-0.cambridge2-br2.bbnplanet.net (4.0.1.202)  62 ms  55 ms  55 ms
10 ihtfp.mit.edu (192.233.33.3)  59 ms  54 ms  57 ms
11 W20-RTR-FDDI.MIT.EDU (18.168.0.8)  58 ms  56 ms  54 ms
12 DANDELION-PATCH.MIT.EDU (18.181.0.31)  59 ms  *  56 ms
```

Détermination de la MTU de chemin

- Objectif : éviter la fragmentation des datagrammes (impact sur les performances), en limitant au mieux leur taille
- MTU de chemin : valeur de MTU la plus faible le long du chemin entre une source et une destination
- Test de la MTU de chemin par envoi de datagrammes avec flag **DF** *(Don't Fragment)* activé :
  - ✓ si datagramme trop grand, réception d'un message **ICMP de destination inaccessible**
  - ✓ nouveau test avec message plus court, etc.
- Remarques :
  - ✓ routes relativement stables
  - ✓ amélioration de cette technique avec IPv6 : recherche de MTU de chemin obligatoire (pas de fragmentation dans les routeurs)