

Les protocoles de couche réseau ARP/RARP

Les protocoles de couche réseau ARP/RARP – Sommaire

Les protocoles de couche réseau ARP/RARP

Routage direct et indirect

Protocoles ARP et RARP

Principe de résolution d'adresses ARP

arp

Routage direct et indirect

Objectif d'un routeur suivant les formes de routage

- **Routage indirect** : Déterminer **le routeur** auquel il faut envoyer le datagramme à partir du numéro réseau de l'adresse IP
- **Routage direct** : Machines rattachées sur un même réseau (même numéro de réseau IP)
E.g. 2 hôtes ou 1 hôte et 1 routeur
Déterminer **l'adresse physique** du destinataire et encapsulation du datagramme dans une trame

Protocoles ARP et RARP

Permettent de **faire le lien entre les adresses physiques (MAC) et logiques (IP)** d'une même machine

- **ARP (Address Resolution Protocol)** permet de faire correspondre une adresse MAC à une adresse IP donnée
- Et **RARP (Reverse Address Resolution Protocol)** permet l'inverse
Utilisé lors d'un lancement d'une machine pour demander son IP à un serveur d'adresses

Principe de résolution d'adresses ARP

La résolution d'adresses est effectuée en trois étapes :

1. Le protocole **ARP émet un datagramme particulier qui contient (entre autre) l'adresse IP à convertir, à destination de l'ensemble des stations du réseau**
2. La station **qui se reconnaît retourne un message (réponse ARP) à l'émetteur avec son adresse MAC**
3. L'émetteur dispose alors de l'adresse physique du destinataire et ainsi la couche liaison de données peut émettre les trames directement vers cette adresse physique
Les **adresses résolues sont placées dans un cache** ce qui évite de déclencher plusieurs requêtes lorsque plusieurs datagramme doivent être envoyés

arp

`arp` (sous linux) : consulte, nettoie ou spécifie le cache ARP de la machine locale



```
herandez@tamata: ~  
herandez@tamata:~$ arp -av  
hebus (192.168.1.101) à 00:01:03:8D:F6:6C [ether] sur eth1  
BRN-89EE5C.local (192.168.1.103) à 00:80:77:89:EE:5C [ether] sur eth1  
? (192.168.1.254) à 00:13:46:06:78:8E [ether] sur eth1  
Entrées: 3      Ignorées: 0      Trouvées: 3  
herandez@tamata:~$
```

Le protocole de couche réseau ICMP – Sommaire

Le protocole de couche réseau ICMP

Objectif et Format ICMP

ping

Exemple d'utilisation d'ICMP : traceroute

Autre exemple d'utilisation d'ICMP : information de routage

Le protocole de couche réseau ICMP

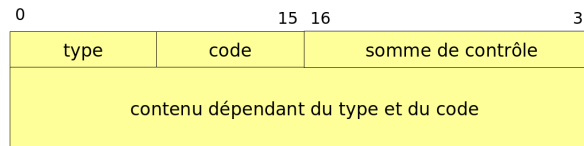
Objectif et Format ICMP

ping

Exemple d'utilisation d'ICMP : traceroute

Autre exemple d'utilisation d'ICMP : information de routage

Objectif et Format ICMP



Objectif

ICMP (Internet Control Message Protocol) : Permet de signaler les erreurs de transmission des paquets

Règle : **ne jamais générer un message d'erreur ICMP pour**

- en réponse à un autre message ICMP (exception requêtes ICMP)
- un paquet destiné à une adresse broadcast
- un paquet dont l'expéditeur n'a pas une adresse unique (adresse zéro, bouclage, adresse broadcast)
- un fragment autre que le premier

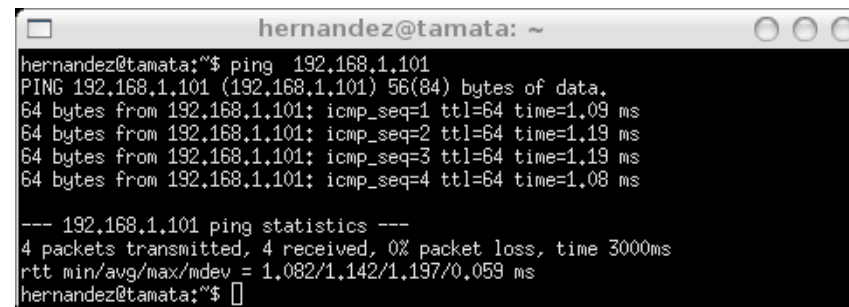
Type et code des paquets ICMP

| type | code | description |
|------|------|--------------------------------|
| 0 | 0 | réponse echo (ping) |
| 3 | | destination inaccessible |
| | 0 | réseau inaccessible |
| | 1 | machine inaccessible |
| | 2 | protocole inaccessible |
| | 3 | port inaccessible |
| | 4 | fragmentation nécessaire |
| | 5 | échec de la route source |
| | 6 | réseau de destination inconnue |
| 4 | 0 | débit trop élevé |
| 5 | 0 | redirigé |
| 8 | 0 | requête echo (ping) |

| type | code | description |
|------|------|------------------------------------|
| 9 | 0 | avertissement du routeur |
| 10 | 0 | sollicitation du routeur |
| 11 | | temps dépassé: |
| | 0 | TTL vaut 0 pendant le transit |
| | 1 | TTL vaut 0 pendant le réassemblage |
| 12 | | problème de paramètre |
| | 0 | mauvaise entête IP |
| | 1 | option requise manquante |
| 13 | 0 | requête timestamp |
| 14 | 0 | réponse timestamp |
| 17 | 0 | requête de masque d'adresse |
| 18 | 0 | réponse du masque d'adresse |

ping

ping - send ICMP ECHO_REQUEST to network hosts



```
herandez@tamata: ~  
herandez@tamata:~$ ping 192.168.1.101  
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.  
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=1.09 ms  
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=1.19 ms  
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=1.19 ms  
64 bytes from 192.168.1.101: icmp_seq=4 ttl=64 time=1.08 ms  
  
--- 192.168.1.101 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3000ms  
rtt min/avg/max/mdev = 1.082/1.142/1.197/0.059 ms  
herandez@tamata:~$
```

(ici interrompu avec un CTRL +C)

Le protocole de couche réseau ICMP

Objectif et Format ICMP

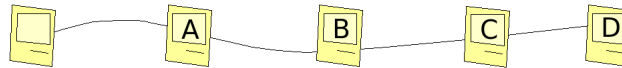
ping

Exemple d'utilisation d'ICMP : traceroute

Autre exemple d'utilisation d'ICMP : information de routage

Exemple d'utilisation d'ICMP : traceroute

traceroute IP-de-D : identification des noeuds intermédiaires jusqu'à D



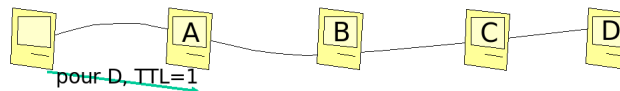
Tout paquet IP a un champs Time To Live qui est décrémenté à chaque passage par un routeur

TTL=0 → le packet est détruit, un message ICMP en avverti l'émetteur

...

Exemple d'utilisation d'ICMP : traceroute

traceroute IP-de-D : identification des noeuds intermédiaires jusqu'à D



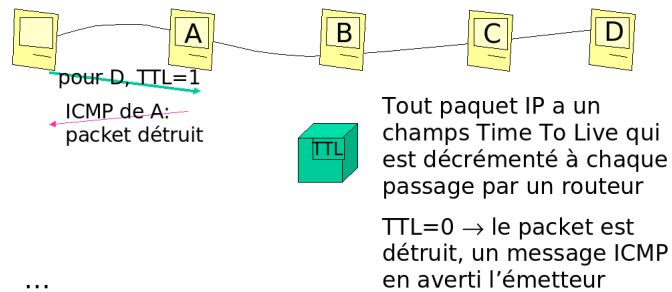
Tout paquet IP a un champs Time To Live qui est décrémenté à chaque passage par un routeur

TTL=0 → le paquet est détruit, un message ICMP en avverti l'émetteur

...

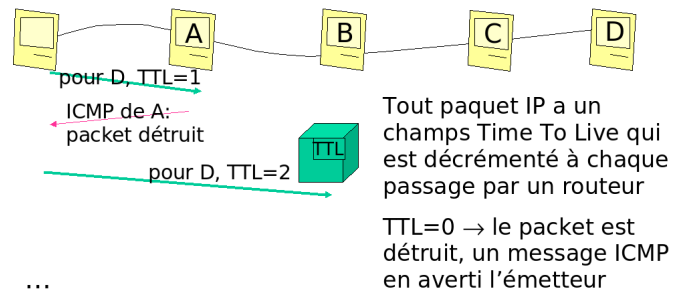
Exemple d'utilisation d'ICMP : traceroute

traceroute IP-de-D : identification des noeuds intermédiaires jusqu'à D



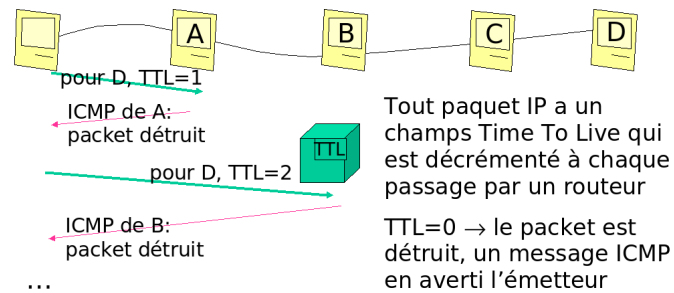
Exemple d'utilisation d'ICMP : traceroute

traceroute IP-de-D : identification des noeuds intermédiaires jusqu'à D



Exemple d'utilisation d'ICMP : traceroute

traceroute IP-de-D : identification des noeuds intermédiaires jusqu'à D



Autre exemple d'utilisation d'ICMP : information de routage

un routeur informe un autre présent sur le même réseau local qu'une meilleure route existe pour joindre un tiers

