

Chapitre III Adressage (Couche Internet et Couche Liaison) Partie 3- Internet Control Message Protocol

Ilyas Bambrik

Table des matières



I - Internet Control Message Protocol (ICMP)	3
II - Structure du message ICMP	4
III - Echo Request (Type ==8) et Echo Reply (Type ==0)	5
IV - ICMP Time Exceeded (Type ==11)	7
V - ICMP Destination Unreachable (Type ==3)	10
VI - ICMP Redirect (Type ==5)	12

Internet Control Message Protocol (ICMP)



- Internet Control Message Protocol (ICMP) est un protocole permettant de diagnostiquer le fonctionnement du réseau et de signaler des erreurs de routage ;
- ICMP fonctionne au niveau de la Couche Internet du modèle TCP / IP ;
- Plusieurs commandes utilisent ICMP pour fonctionner (ping, tracert / traceroute).
- Les messages générés par ce protocole sont encapsulés par un entête IP. Si dans un message IPv4 la *valeur du champs Protocol est égale à 1*, le message encapsulé est un message ICMP ;
- La plus part des machines fonctionnant sur Internet sont configurées pour répondre aux messages ICMP (comme ping par exemple);

Structure du message ICMP



- La structure du message ICMP change selon la valeur du champ *type*;
- Les champs suivants qui peuvent être présents dans un message ICMP sont :
 1. *Type [présent dans tous les messages ICMP]*: Valeur numérique qui indique le type du message ICMP. Il existe 16 types de messages ICMP mais ceux fréquemment rencontrés sont :
 - 0—Echo reply
 - 3—Destination unreachable
 - 5—Redirect
 - 8—Echo request
 - 11—Time Exceeded
 2. *Code [présent dans tous les messages ICMP]*: La valeur du code prend souvent 0. Si ce champ prend une valeur différent de 0, cela indique que le message ICMP représente une variation d'un type de message (*champ 1*). Pour les messages ICMP qui n'ont pas de variantes, le champ *code* prends toujours la valeur 0 ;
 3. *Checksum [présent dans tous les messages ICMP]*: Valeur de contrôle du message ICMP entier ;
 4. *Identifiant* : N'est pas présent dans tous les types de messages ICMP. Cette valeur peut faire référence à un message ICMP précédant qui a provoqué l'envoi de ce message ICMP ;
 5. *Numéro de séquence* : Comme l'identifiant, la valeur de ce champ est utilisée pour faire la correspondance entre le *Echo Request* et le *Echo Reply* ;
 6. *Copie de l'entête IP + copie de 64 bits des données encapsulées (8 octets)* : Ce champs est présent dans certains types de message ICMP pour faire référence au message qui a provoqué la génération de ce dernier ;
 7. *Payload*: Les données enveloppées par le message ICMP ;

Echo Request (Type ==8) et Echo Reply (Type ==0)

III

- La commande *ping* présente sur Windows et Linux génère un message *ICMP Echo Request (Type == 8)* ;
- Le destinataire qui correspond à l'adresse IP fournie répond avec un message *ICMP Echo Reply (Type == 0)*;
- Le payload d'un message Echo Request contient une suite d'octets. Les octets insérés dans ce champ dépendent du système d'exploitation. Par exemple : Windows génère un payload de 32 octets contenant des caractères alphabétiques (de 'a' jusqu'à 'z' et ensuite de 'a' jusqu'à 'i'), Ubuntu génère une suite de 48 octets avec une suite de caractères différente ;
- Le Echo Reply correspondant à un Echo Request aura la même valeur d'identification, le même numéro séquence et la même suite d'octets constituant le payload ;

```

No.    Time    Source        Destination    Protocol Length Info
--
4 15.126540 192.168.1.3  192.168.1.2  ICMP      74 Echo (ping) request id=0x0001, seq=391/34561, ttl=128 (reply in 5)
5 15.189381 192.168.1.2  192.168.1.3  ICMP      74 Echo (ping) reply id=0x0001, seq=391/34561, ttl=64 (request in 4)
7 16.138463 192.168.1.3  192.168.1.2  ICMP      74 Echo (ping) request id=0x0001, seq=392/34817, ttl=128 (no response found!)
8 16.208950 192.168.1.2  192.168.1.3  ICMP      74 Echo (ping) reply id=0x0001, seq=392/34817, ttl=64 (request in 7)

> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_d4:c7:1d (48:51:b7:d4:c7:1d), Dst: 00:d5:76:de:15:5c (00:d5:76:de:15:5c)
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.2
> Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4bd4 [correct]
  [Checksum Status: Good]
  Identifiant (BE): 1 (0x0001)
  Identifiant (LE): 256 (0x0100)
  Sequence number (BE): 391 (0x0187)
  Sequence number (LE): 34561 (0x8701)
  [Response time: ...]
  > Data (32 bytes)

0000  00 d5 76 de 15 5c 48 51 b7 d4 c7 1d 08 00 45 00  ..v..HQ .....E.
0010  00 3c 2f 2c 00 00 80 01 88 3f c0 a8 01 03 c0 a8  </.....?.....
0020  01 02 08 00 4b d4 00 01 01 87 61 62 63 64 65 66  ...K... abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

Identification et numéro de séquence d'un Echo request

Payload d'un ICMP Echo request

Figure 1. Echo Request

```

No.    Time    Source        Destination    Protocol Length Info
--
4 15.126540 192.168.1.3  192.168.1.2  ICMP      74 Echo (ping) request id=0x0001, seq=391/34561, ttl=128 (reply in 5)
5 15.189381 192.168.1.2  192.168.1.3  ICMP      74 Echo (ping) reply id=0x0001, seq=391/34561, ttl=64 (request in 4)
7 16.138463 192.168.1.3  192.168.1.2  ICMP      74 Echo (ping) request id=0x0001, seq=392/34817, ttl=128 (no response found!)
8 16.208950 192.168.1.2  192.168.1.3  ICMP      74 Echo (ping) reply id=0x0001, seq=392/34817, ttl=64 (request in 7)

> Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: 00:d5:76:de:15:5c (00:d5:76:de:15:5c), Dst: IntelCor_d4:c7:1d (48:51:b7:d4:c7:1d)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.3
> Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x53d4 [correct]
  [Checksum Status: Good]
  Identifiant (BE): 1 (0x0001)
  Identifiant (LE): 256 (0x0100)
  Sequence number (BE): 391 (0x0187)
  Sequence number (LE): 34561 (0x8701)
  [Request frame: 4]
  [Response time: 62.841 ms]
  > Data (32 bytes)

0000  48 51 b7 d4 c7 1d 00 d5 76 de 15 5c 08 00 45 00  HQ..... v...E.
0010  00 3c 1b ce 00 00 40 01 db 9d c0 a8 01 02 c0 a8  @.....
0020  01 03 00 00 53 d4 00 01 01 87 61 62 63 64 65 66  ...S... abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

Identification et numéro de séquence d'un Echo reply

Payload d'un Echo reply

Figure 2. Echo Reply

 **Remarque : Identification et numéro de séquence**

Wireshark affiche l'identification et le numéro de séquence d'un message ICMP sous deux formats (BE == Big Endian , LE == Little Endian).

ICMP Time Exceeded (Type ==11)

IV

- Dans le cas où un paquet encapsulé avec un entête IP est supprimé à cause de l'expiration du TTL (TTL == 0), le routeur qui supprime le paquet transmet un *message ICMP avec Time Exceeded (Type == 11)* vers la source du paquet supprimé ;
- Ceci informe la source que le paquet a potentiellement traversé une boucle de routage (routing loop) ;
- Contrairement à Echo reply / request, un message ICMP Time Exceeded ne contient pas le champ identification / numéro de séquence. Ce type de message contient une copie du message qui a expiré (TTL a atteint 0) ;
- Le deuxième cas d'utilisation pour Time Exceeded c'est lorsque un fragment est perdu/supprimé ainsi le reste des fragments ne peuvent pas être livrés à la couche transport. Dans ce cas, un message *Time Exceeded (Type == 11)* avec code =1 est envoyé (Temps de ré-assemblage des fragments du datagramme dépassé) ;

Remarque : TTL

-
- Chaque fois qu'un paquet est retransmis par un routeur, la valeur du TTL est décrémentée par au moins 1. Dans certaines situations, le TTL est décrémenté par une valeur supérieure ;
 - La commande *Tracert* (traceroute sur Linux) utilise ICMP Time Exceeded pour retrouver les sauts sur le chemin vers la destination. La source transmet des messages *ICMP Echo Request avec des TTL incrémentés* de 1 jusqu'à ce que la source est atteinte. La transmission d'un echo request avec un TTL ==N permet de traverser N sauts seulement (car la machine positionnée dans le saut numéro N supprimera le paquet puisque le TTL initial a été décrémenté N fois au moins pour l'atteindre). Chaque fois qu'une machine sur la route supprime le message à cause de l'expiration du TTL, elle renvoie un ICMP Time Exceeded vers la source. Ainsi, la source détermine le générateur du ICMP Type ==11 est positionnée sur la route à la *N^{em} position* ;
 - Lorsque l'administrateur réseau souhaite qu'une machine ne soit pas visible dans la route tracée par cette commande, il suffit de configurer celle-ci pour ne pas décrémenter le TTL

No.	Time	Source	Destination	Protocol	Length	Info
71	29.564538	192.168.1.4	172.217.19.131	ICMP	106	Echo (ping) request id=0x0001, seq=80/20480, ttl=4 (no response found!)
72	29.592381	172.28.16.13	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
83	35.188809	192.168.1.4	172.217.19.131	ICMP	106	Echo (ping) request id=0x0001, seq=81/20736, ttl=5 (no response found!)
84	35.213918	172.28.16.14	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 71: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
 > Ethernet II, Src: IntelCor_d4:c7:1d (48:51:b7:d4:c7:1d), Dst: HuaweiTe_6d:c1:aa (00:66:4b:6d:c1:aa)
 > Internet Protocol Version 4, Src: 192.168.1.4, Dst: 172.217.19.131
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xf7ae [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence number (BE): 80 (0x0050)
 Sequence number (LE): 20480 (0x5000)
 > [No response seen]

Echo request avec TTL==4

Message original

> Data (64 bytes)
 Data: 00...
 [Length: 64]

No.	Time	Source	Destination	Protocol	Length	Info
71	29.564538	192.168.1.4	172.217.19.131	ICMP	106	Echo (ping) request id=0x0001, seq=80/20480, ttl=4 (no response found!)
72	29.592381	172.28.16.13	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
83	35.188809	192.168.1.4	172.217.19.131	ICMP	106	Echo (ping) request id=0x0001, seq=81/20736, ttl=5 (no response found!)
84	35.213918	172.28.16.14	192.168.1.4	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

> Frame 72: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
 > Ethernet II, Src: HuaweiTe_6d:c1:aa (00:66:4b:6d:c1:aa), Dst: IntelCor_d4:c7:1d (48:51:b7:d4:c7:1d)
 > Internet Protocol Version 4, Src: 172.28.16.13, Dst: 192.168.1.4
 > Internet Control Message Protocol
 Type: 11 (Time-to-live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0xf4ff [correct]
 [Checksum Status: Good]

ICMP Type 11 avec l'adresse du 4em saut

> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 172.217.19.131
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0xf7ae [unverified] [in ICMP error packet]
 [Checksum Status: Unverified]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence number (BE): 80 (0x0050)
 Sequence number (LE): 20480 (0x5000)

Copie du message original qui a engendré le message ICMP Type 11

```
(c) 2018 Microsoft Corporation. Tous droits réservés.
C:\Users\DVR>tracert google.dz
Détermination de l'itinéraire vers google.dz [172.217.19.131]
avec un maximum de 30 sauts :

  1  1 ms <1 ms <1 ms 192.168.1.1
  2 16 ms 15 ms 15 ms
  3 22 ms 20 ms 21 ms
  4 28 ms 28 ms 28 ms 172.28.16.13
  5 25 ms 25 ms 25 ms 172.28.16.14
  6 25 ms 24 ms 24 ms 172.17.116.16
  7 43 ms 43 ms 42 ms 72.14.205.138
  8 48 ms 49 ms 48 ms 108.170.252.225
  9 51 ms 51 ms 52 ms 66.249.94.127
 10 42 ms 42 ms 42 ms par03s12-in-f131.1e100.net [172.217.19.131]

Itinéraire déterminé.
C:\Users\DVR>
```

Figure 4. Fonctionnement de la commande Tracert

👉 Exemple : Boucle de routage

Par exemple, Routeur 3 a une route manuellement configurée vers le réseau 192.168.1.0 et Routeur 2 est configuré avec le Routeur 3 comme route par défaut. Si la route vers 192.168.1.0 est supprimée de Routeur 2 à cause d'une panne, lorsque Routeur 3 souhaite communiquer avec 192.168.1.0, une boucle de routage se formera : car Routeur 3 utilise Routeur 2 pour atteindre 192.168.1.0, et Routeur 2 n'a pas de route vers 192.168.1.0 et donc utilisera la route par défaut (Routeur 3). Ainsi, Routeur 2 et Routeur 3 s'échangeront le message destiné au réseau 192.168.1.0 jusqu'à ce que le TTL du paquet atteindra 0 et un message ICMP Type 11 est transmis vers la source de cette transmission ;

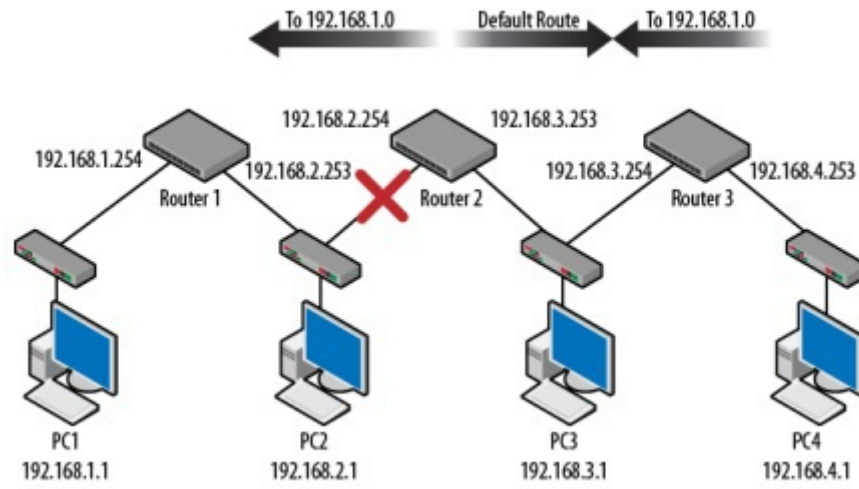


Figure 3. Boucle de routage [*Packet Guide to Core Network Protocols*]

ICMP Destination Unreachable (Type ==3)



Un message ICMP de type 3 est généré quand le paquet ne trouve pas une route correspondante à la destination ou ne peut pas être transmis vers celle-ci. Les codes (*variations*) suivants possibles pour ce type de message sont :

- 0—*Net unreachable* : Le réseau n'est pas atteignable ;
- 1—*Host unreachable* : La machine n'est pas atteignable ;
- 2—*Protocol unreachable* : Le protocole de transport utilisé n'est pas supporté ;
- 3—*Port unreachable* : La destination n'a pas de service correspondant au numéro de port et il n'y a pas un mécanisme pour informer la source (*comme c'est le cas pour UDP !*);
- 4—*Fragmentation needed and DF (do not fragment) set* : Le paquet ne peut pas être transmis car Do Not Fragment == 1 et la fragmentation a été requise ;
- 5—*Source route failed* : Le message original utilise Source Routing et cette option est bloquée par le routeur ;
- 13—*Communication administratively filtered* : Le paquet a été bloqué à cause d'un filtre administrative basé sur le contenu (par exemple le firewall [*pare-feu*] est configuré pour bloquer les paquets destinés au port 137) ;

No.	Time	Source	Destination	Protocol	Length	Info
23259	294.653027	192.168.1.2	10.103.13...	TCP	66	51363 → 23 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
23260	294.670017	10.103.13...	192.168.1.2	ICMP	70	Destination unreachable (Communication administratively filtered)
23270	297.653342	192.168.1.2	10.103.13...	TCP	66	[TCP Retransmission] 51363 → 23 [SYN] Seq=0 Win=17520 Len=0 MSS=1460

```

> Frame 23260: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: HuaweiTe_6d:c1:aa (00:66:4b:6d:c1:aa), Dst: IntelCor_d4:c7:1d (48:51:b7:d4:c7:1d)
> Internet Protocol Version 4, Src: 10.103.13.45, Dst: 192.168.1.2
  > Internet Control Message Protocol
    > Type: 3 (Destination unreachable)
      Code: 13 (Communication administratively filtered)
      Checksum: 0x38d4 [correct]
      [Checksum Status: Good]
      Unused: 00000000
    > Internet Protocol Version 4, Src: 192.168.1.2, Dst: 10.103.13.45
    > Transmission Control Protocol, Src Port: 51363, Dst Port: 23
  
```

Figure 5. Communication administratively filtered

Chacun de ces messages ICMP type 3 contient une copie de l'entête et du payload [*champ 7 du message ICMP*] du message que le routeur a échoué de livrer.

Filter: udp.port==5000 || icmp.type==3

No.	Time	Source	Destination	Protocol	Length	Info
3754	67.774863	192.168.1.2	192.168.1.1	UDP	81	60774 → 5000 Len=39
3755	67.775662	192.168.1.1	192.168.1.2	ICMP	109	Destination unreachable (Port unreachable)

Checksum: 0x12dd [unverified]
 [Checksum Status: Unverified]
 [Stream index: 9]

▼ Data (39 bytes)
 Data: 4579203139322e3136382e312e31212074752065636f7574...

```

0000  00 66 4b 6d c1 aa 48 51 b7 d4 c7 1d 08 00 45 00  .fKm..HQ.....E.
0010  00 43 79 34 00 00 80 11 3e 22 c0 a8 01 02 c0 a8  .Cy4....>.....
0020  01 01 ed 66 13 88 00 2f 12 dd 45 79 20 31 39 32  ...f.../..Ey 192
0030  2e 31 36 38 2e 31 2e 31 21 20 74 75 20 65 63 6f  .168.1.1! tu eco
0040  75 74 65 20 6c 65 20 70 6f 72 74 20 35 30 30 30  ute le p ort 5000
0050  3f
    
```

> Frame 3755: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
 > Ethernet II, Src: HuaweiTe_6d:c1:aa (00:66:4b:6d:c1:aa), Dst: IntelCor_d4:c7:1d (48:51:b7:d4:c7:1d)
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
 ▼ Internet Control Message Protocol
 Type: 3 (Destination unreachable)
 Code: 3 (Port unreachable)
 Checksum: 0x8091 [correct]
 [Checksum Status: Good]
 Unused: 00000000
 > Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1 Copie de l'entete
 > User Datagram Protocol, Src Port: 60774, Dst Port: 5000
 ▼ Data (39 bytes)
 Data: 4579203139322e3136382e312e31212074752065636f7574...

```

0000  48 51 b7 d4 c7 1d 00 66 4b 6d c1 aa 08 00 45 c0  HQ.....f Km....E.
0010  00 5f 81 06 00 00 40 01 75 84 c0 a8 01 01 c0 a8  _...@. u.....
0020  01 02 03 03 80 91 00 00 00 00 45 00 00 43 79 34  .....E..Cy4
0030  00 00 80 11 3e 22 c0 a8 01 02 c0 a8 01 01 ed 66  >.....f
0040  13 88 00 2f 12 dd 45 79 20 31 39 32 2e 31 36 38  .../..Ey 192.168
0050  2e 31 2e 31 21 20 74 75 20 65 63 6f 75 74 65 20  .1.1! tu ecoute
0060  6c 65 20 70 6f 72 74 20 35 30 30 30 3f  le port 5000?
    
```

Figure 6. Message ICMP Type ==3 Code ==3

Remarque : Traceroute sur Linux

Alors que `tracert` sur Windows utilise `echo request` et `ICMP TTL Exceeded`, la commande Traceroute sur Linux génère des `datagrames UDP` avec un TTL progressivement incrémenté et attend de recevoir le message ICMP TTL Exceeded par les machines intermédiaires. La destination finale répondra généralement avec un ICMP Destination Unreachable (Type 3) Port Unreachable (Code 3).

ICMP Redirect (Type ==5)

VI

Un message ICMP Redirect (Type ==5) est généré pour informer la source d'un paquet que sa destination est joignable par un plus court chemin *dans le même réseau*. Ainsi, le routeur qui génère un paquet ICMP Redirect envoie la nouvelle route vers la source. Ensuite, la source ajoute une nouvelle entrée dans sa table de routage vers la destination souhaitée avec le prochain saut égale à la route spécifiée par le ICMP Redirect.

☞ Exemple : Exemple scénario ICMP Redirect

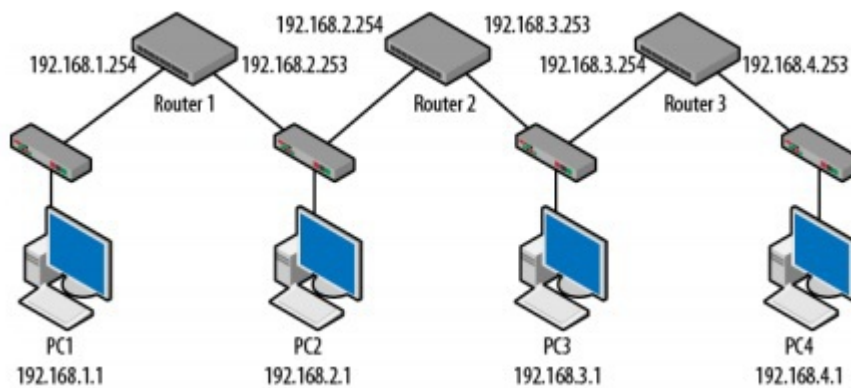


Figure 7. Exemple ICMP Redirect [Packet Guide to Core Network Protocols]

- Dans l'exemple présenté dans *Figure 7*, PC3 est configuré avec Router 2 comme route par défaut et ne connaît pas de route vers le réseau 192.168.4.0 (où PC4 se trouve). En outre, *Router 2 connaît toutes les routes vers les réseaux atteignables*. Ainsi, quand PC 3 souhaite transmettre des paquets vers PC4, celui-ci utilise Router 2.
- Router 2 détermine que PC3 possède une route plus courte vers PC4 (car *pour Router 2 le prochain saut vers 192.168.4.0 est Router 3 && Router 3 et PC3 sont dans le même réseau*). Ainsi, *Router 2 envoie un message ICMP Redirect vers PC3 pour lui dire qu'il peut rejoindre PC4 à travers Router 3* ;

Si la route est explicitement définie par la source (*Source Routing est appliqué*), le routeur ne génère pas de ICMP Redirect même s'il y a une meilleure route ;