

Exonet N°82 : Comprendre le rôle du protocole ICMP

Propriétés	Description
Intitulé long	Comprendre le rôle du protocole ICMP (<i>Internet Control Message Protocol</i>) dans les échanges d'informations de contrôle et de gestion du réseau.
Formation concernée	BTS Informatique de gestion option Administrateur de réseaux locaux d'entreprise.
Matière	Architecture matérielle des systèmes informatiques.
Présentation	Analyser le dialogue ICMP sur un réseau, en déduire le fonctionnement du protocole.
Notions	S15 Architecture des réseaux C22 Installer et configurer un réseau C34 Surveiller et optimiser le trafic sur un réseau
Pré-requis	Adresse Mac, adresse IP, trame, table de routage, passerelle
Outils	Un logiciel analyseur de trames si on souhaite analyser un dialogue ICMP réel
Mots-clés	TCP/IP ICMP routage ping
Durée indicative	2 heures
Auteur(es)	Daniel Regnier et l'équipe ARLE du Certa pour la relecture.
Version	v 1.0
Date de publication	18 janvier 2006

Exonet N°82 : Comprendre le rôle du protocole ICMP

Énoncé

L'administrateur réseau d'une entreprise étudie la configuration IP des postes d'un réseau situé entre deux autres réseaux (voir le schéma du réseau en **annexe 1**).

Il cherche à optimiser l'utilisation des routeurs R1 et R2 (**annexe 2**) en fonction de la destination des paquets émis par les postes du réseau IP intermédiaire. Pour cela il veut s'appuyer sur les services offerts par le protocole ICMP (**annexe 3** : document ICMP-RFC.DOC).

Mais avant d'arrêter sa décision sur le choix de la passerelle par défaut, il souhaite étudier le fonctionnement du protocole ICMP dans différents cas de configuration.

L'administrateur utilise le poste P2 pour ses tests. Un analyseur de trames fonctionnant en mode « promiscus » a été installé sur ce dernier. Ce mode permet au logiciel de capturer toutes les trames reçues par la carte réseau dans une architecture non commutée.

L'administrateur a testé quatre configurations.

1. Première configuration

Il n'y a pas de passerelle par défaut définie sur le poste P2.

L'administrateur lance, à partir du poste P2, la commande suivante : **PING 192.168.0.10**

Il obtient la réponse :

Impossible de joindre l'hôte de destination

Aucune trame n'a été capturée par le logiciel.

Questions

1.1 Justifier le message obtenu.

1.2 Justifier l'absence de trames capturées.

2. Deuxième configuration

L'administrateur ajoute sur P2, l'adresse de passerelle par défaut suivante : 192.168.100.2.

L'administrateur lance, à partir du poste P2, la commande suivante : **PING 192.168.0.10**

Il obtient la réponse :

Réponse de 192.168.100.2 : impossible de joindre l'hôte de destination

Les champs ICMP des trames capturées sont les suivants :

Trame 1

Adresse Ethernet destination : 00 03 FF **40** 6C 35

Adresse Ethernet source : 00 03 FF **4B** 6C 35

Ip source : 192.168.100.10

Ip destination : 192.168.0.10

Champs ICMP (hexa) :

08	00	3A	5C
02	00	11	00
...

Trame 2

Adresse Ethernet destination : 00 03 FF **4B** 6C 35

Adresse Ethernet source : 00 03 FF **40** 6C 35

Ip source : 192.168.100.2

Ip destination : 192.168.100.10

Champs ICMP (hexa) :

03	01	A7	A2
00	00	00	00
...
08	00	3A	5C
02	00	11	00

Questions

- 2.1 Justifier les valeurs des adresses MAC de la trame n°1.
- 2.2 Indiquer quelle trame capturée a transporté le message obtenu ?
- 2.3 Justifier le message obtenu : « Impossible de joindre l'hôte de destination ».

3. Troisième configuration

L'administrateur ajoute sur R2, la route suivante (ligne 3) dans la table de routage :

	Réseau	Masque	Passerelle	Interface
1	192.168.100.0	255.255.255.0	192.168.100.2	192.168.100.2
2	192.168.200.0	255.255.255.0	192.168.200.2	192.168.200.2
3	192.168.0.0	255.255.255.0	192.168.100.1	192.168.100.2

L'administrateur lance, à partir du poste P2, la commande suivante : **PING 192.168.0.10**

Il obtient la réponse :

Réponse de 192.168.0.10 : octets=32 temps=40ms TTL=127

Réponse de 192.168.0.10 : octets=32 temps=10ms TTL=127

Questions

A l'aide des extraits de captures de trame en **Annexe 4**

- 3.1 Donner la valeur décimale des octets 5 à 8 des champs ICMP de la trame n° 2.
- 3.2 Expliquer le rôle de la trame n°2.
- 3.3 Justifier les valeurs de l'adresse MAC source et de l'adresse IP source de la trame n° 3.
- 3.4 Expliquer le rôle des trames 5 et 6.
- 3.5 Justifier la différence des temps affichés entre le premier et le deuxième message ICMP.

4. Quatrième configuration

Cette configuration a été créée dynamiquement par le test effectué précédemment. Le système d'exploitation utilisé permet d'afficher cette configuration dynamique.

Extrait de la table de routage de P2 à l'issue du test de la troisième configuration :

	Réseau	Masque	Passerelle	Interface
1	192.168.0.10	255.255.255.255	192.168.100.1	192.168.100.10
2	192.168.100.10	255.255.255.255	127.0.0.1	127.0.0.1
3	192.168.100.0	255.255.255.0	192.168.100.10	192.168.100.10
..
..	0.0.0.0	0.0.0.0	192.168.100.2	192.168.100.10

L'administrateur lance, à partir du poste P2, la commande suivante : **PING 192.168.0.10**

Il obtient la réponse :

Réponse de 192.168.0.10 : octets=32 temps=10ms TTL=127

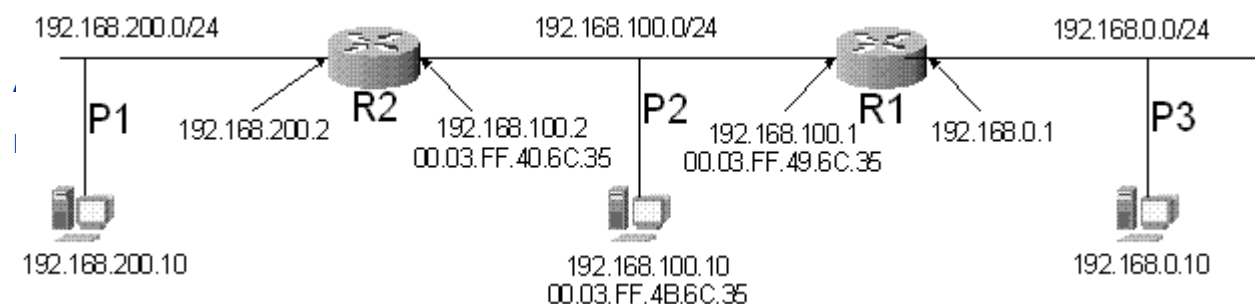
Réponse de 192.168.0.10 : octets=32 temps=10ms TTL=127

Questions

- 4.1 Justifier la dernière ligne de la table de routage de P2.
- 4.2 Justifier la première ligne de la table de routage de P2.
- 4.3 Justifier le masque utilisé sur la première ligne.
- 4.4 Donner l'entête MAC et IP des deux premières trames capturées dans cet échange

Annexes

Annexe 1 : schéma du réseau



	Réseau	Masque	Passerelle	Interface
1	192.168.100.0	255.255.255.0	192.168.100.1	192.168.100.1
2	192.168.0.0	255.255.255.0	192.168.0.1	192.168.0.1

Routeur R2

	Réseau	Masque	Passerelle	Interface
1	192.168.100.0	255.255.255.0	192.168.100.2	192.168.100.2
2	192.168.200.0	255.255.255.0	192.168.200.2	192.168.200.2

Annexe 3 : Extrait de la RFC 792 : Internet Control Message Protocol (ICMP)

En français, adapté du document : <http://abcdrfc.free.fr/rfc-vf/rfc792.html>

Original en anglais sur le site : <http://www.rfc-editor.org>

À l'adresse : <ftp://ftp.rfc-editor.org/in-notes/rfc792.txt>

Voir document ICMP-RFC du réseau Certa dans l'archive

Annexe 4 : champs ICMP des trames capturées pour la troisième configuration

Trame 1

Adresse Ethernet destination : 00 03 FF **40** 6C 35
Adresse Ethernet source : 00 03 FF **4B** 6C 35
Ip source : 192.168.100.10
Ip destination : 192.168.0.10

Champs ICMP (hexa) :

08	00	2E	5C
02	00	1D	00
...

Trame 2

Adresse Ethernet destination : 00 03 FF **4B** 6C 35
Adresse Ethernet source : 00 03 FF **40** 6C 35
Ip source : 192.168.100.2
Ip destination : 192.168.100.10

Champs ICMP (hexa) :

05	01	80	F8
C0	A8	64	01
...
08	00	2E	5C
02	00	1D	00

Trame 3

Adresse Ethernet destination : 00 03 FF **49** 6C 35
Adresse Ethernet source : 00 03 FF **40** 6C 35
Ip source : 192.168.100.10
Ip destination : 192.168.0.10

Champs ICMP (hexa) :

08	00	2E	5C
02	00	1D	00
...

Trame 4

Adresse Ethernet destination : 00 03 FF **4B** 6C 35
Adresse Ethernet source : 00 03 FF **49** 6C 35
Ip source : 192.168.0.10
Ip destination : 192.168.100.10

Champs ICMP (hexa) :

00	00	36	5C
02	00	1D	00
...

Trame 5

Adresse Ethernet destination : 00 03 FF **49** 6C 35
Adresse Ethernet source : 00 03 FF **4B** 6C 35
Ip source : 192.168.100.10
Ip destination : 192.168.0.10

Champs ICMP (hexa) :

08	00	2D	5C
02	00	1E	00
...

Trame 6

Adresse Ethernet destination : 00 03 FF **4B** 6C 35
Adresse Ethernet source : 00 03 FF **49** 6C 35
Ip source : 192.168.0.10
Ip destination : 192.168.100.10

Champs ICMP (hexa) :

00	00	35	5C
02	00	1E	00

Proposition de corrigé

1. Première configuration

1.1 Justifier le message obtenu.

Le poste P2, d'adresse IP 192.168.100.10, n'a pas les éléments dans sa table de routage pour atteindre l'adresse IP 192.168.0.10. Notamment, il n'a pas de passerelle par défaut.

Remarque : Avec Mandrake Linux, le message est : Network is unreachable

1.2 Justifier l'absence de trames capturées.

Le poste P2 n'ayant pas dans sa table de routage les éléments pour atteindre l'adresse IP 192.168.0.10, il ne transmet aucune trame sur le réseau.

2. Deuxième configuration

2.1 Justifier les valeurs des adresses MAC de la trame n°1.

Adresse Ethernet destination : 00 03 FF **40** 6C 35

C'est l'adresse MAC de l'interface (192.168.100.2) du routeur R2 qui est la passerelle par défaut du poste P2. On peut prendre comme hypothèse que cette adresse MAC a été obtenue par une précédente requête ARP.

Adresse Ethernet source : 00 03 FF **4B** 6C 35

C'est l'adresse MAC de l'interface du poste P2.

2.2 Indiquer quelle trame capturée a transporté le message obtenu ?

Trame 1 : C'est le message ICMP "**echo**" (08) transmis par le poste **P2** (00 03 FF **4B** 6C 35) à la passerelle **R2** (00 03 FF **40** 6C 35) à destination de l'Ip 192.168.0.10 (**P3**).

Trame 2 : C'est le message ICMP "**destinataire non accessible**" (03) avec le code "**hôte inaccessible**" (01) transmis par le routeur **R2** (00 03 FF **40** 6C 35) au poste **P2** (00 03 FF **4B** 6C 35)

C'est bien le routeur R2 (192.168.100.2) qui répond que l'hôte est inaccessible dans la trame 2.

2.3 Justifier le message obtenu : « Impossible de joindre l'hôte de destination »..

Le routeur R2, d'adresse IP 192.168.100.2, n'a pas les éléments dans sa table de routage pour atteindre l'adresse IP 192.168.0.10.

Rmq : Avec Mandrake Linux, le message est : From 192.168.100.2 Destination Net Unreachable

3. Troisième configuration

3.1 Donner la valeur décimale des octets 5 à 8 des champs ICMP de la trame n° 2.

$C0 = 12 \times 16 = 192$

$A8 = 10 \times 16 + 8 = 168$

$64 = 6 \times 16 + 4 = 100$

$01 = 1$

Soit : 192.168.100.1

C'est l'adresse IP du routeur R1

3.2 Expliquer le rôle de la trame n°2.

Trame 1 : C'est le message ICMP "**echo**" (08) transmis par le poste **P2** (00 03 FF **4B** 6C 35) à la passerelle **R2** (00 03 FF **40** 6C 35) à destination de l'Ip 192.168.0.10 (**P3**).

Trame 2 : C'est le message ICMP "**de redirection**" (05) avec le code "Redirection de datagramme sur la base de l'adresse d'hôte" (01) transmis par le routeur **R2** (00 03 FF **40** 6C 35) au poste **P2** (00 03 FF **4B** 6C 35).

Ce message contient donc l'adresse IP du routeur R1 qui permet d'atteindre P3 à partir du poste P2 de manière plus directe.

Rmq : Avec Mandrake Linux, le premier message est : From 192.168.100.2 Redirect Host (New nexthop : 192.168.100.1)

3.3 Justifier les valeurs de l'adresse MAC source et de l'adresse IP source de la trame n° 3.

Trame 3 : C'est le message ICMP "**echo**" (08) transmis par le routeur **R2** (00 03 FF **40** 6C 35) au routeur **R1** (00 03 FF **49** 6C 35) à destination de l'Ip 192.168.0.10 (**P3**).

L'adresse MAC source est donc celle de la passerelle qui retransmet le message ICMP au routeur suivant.

L'IP source du message est 192.168.100.10, soit P2, c'est le poste qui est à l'origine du message ICMP "echo".

Conclusion : le routeur R2 a transmis deux messages ICMP, le premier pour signaler au poste P2 une redirection et le second pour transmettre au routeur R1 le message ICMP "echo" de P2.

3.4 Expliquer le rôle des trames 5 et 6.

Trame 5 : C'est le message ICMP "**echo**" (08) transmis par le poste **P2** (00 03 FF **4B** 6C 35) au routeur **R1** (00 03 FF **49** 6C 35) à destination de l'Ip 192.168.0.10 (**P3**).
C'est donc le deuxième message ICMP "echo" de P2.

Trame 6 : C'est le message ICMP "**réponse à echo**" (00) transmis par le routeur **R1** (00 03 FF 49 6C 35) au poste **P2** (00 03 FF **4B** 6C 35) provenant de l'Ip 192.168.0.10 (**P3**).

3.5 Justifier la différence des temps affichés entre le premier et le deuxième message ICMP.

Le premier message a eu un temps de réponse plus élevé car la demande est passée par les deux routeurs R2 et R1, mais la demande suivante est passée directement par R1.

4. Quatrième configuration

4.1 Justifier la dernière ligne de la table de routage de P2.

La dernière ligne correspond à la passerelle par défaut saisie par l'administrateur sur le poste P2.

4.2 Justifier la première ligne de la table de routage de P2.

Cette ligne a été ajoutée de manière dynamique suite au message ICMP "**de redirection**" (05) de la trame N°2. Elle permet d'atteindre l'adresse IP 192.168.0.10 en passant directement par le routeur R1 (192.168.100.1).

4.3 Justifier le masque utilisé sur la première ligne.

L'adresse de la colonne "Réseau" de la première ligne est l'adresse IP du poste P3, soit une adresse de poste, donc tous les bits du masque sont à 1.

4.4 Donner l'entête MAC et IP des deux premières trames capturées dans cet échange.

La table de routage de P2 (ligne 1) permet de ne pas utiliser la passerelle par défaut pour atteindre l'adresse 192.168.0.10. On retrouve donc l'entête MAC et IP des trames 5 et 6.

Soit :

Trame 1 :

Adresse Ethernet destination : 00 03 FF **49** 6C 35
Adresse Ethernet source : 00 03 FF **4B** 6C 35
Ip source : 192.168.100.10
Ip destination : 192.168.0.10

Trame 2 :

Adresse Ethernet destination : 00 03 FF **4B** 6C 35
Adresse Ethernet source : 00 03 FF **49** 6C 35
Ip source : 192.168.0.10
Ip destination : 192.168.100.10