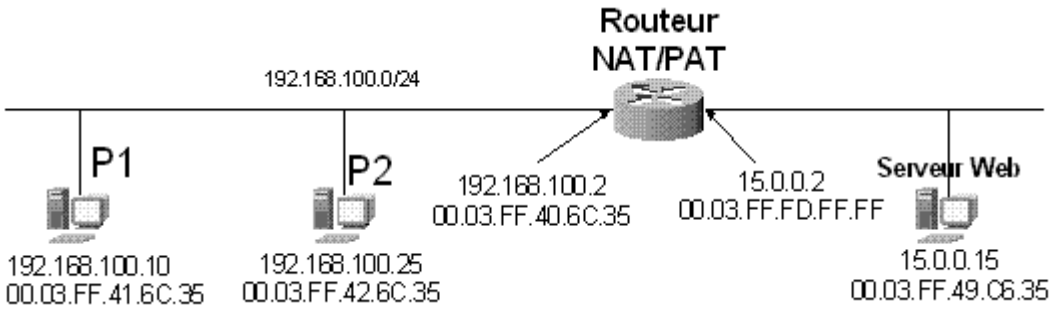
Exercice : Le dialogue ICMP au travers d'un routeur NAT/PAT - TCP/IP ICMP routage ping NAT/PAT

Énoncé

L'administrateur réseau d'une entreprise étudie la mise en place d'un routeur NAT/PAT suivant le schéma ci-dessous :



Le serveur Web est accessible à partir d'Internet à travers un routeur non représenté ici.

Le NAT/PAT est activé sur l'interface 15.0.0.2. L'administrateur réseau veut permettre la communication entre les deux réseaux tout en masquant les adresses du réseau 192.168.100.0.

Il utilise aussi un outil de supervision réseau qui envoie régulièrement des commandes "ping" pour tester l'activité d'un poste
En étudiant précédemment les messages du protocole ICMP (**annexe 1**), il a pu se rendre compte que ce dernier n'utilise pas de port source et de port destination comme les protocoles TCP et UDP.
Le routeur ne fait pas apparaître les échanges ICMP dans sa table de mappage NAT/PAT.
L'administrateur veut étudier l'acheminement des messages ICMP par le routeur NAT/PAT pour contrôler parfaitement les flux. Il décide donc de mettre en place des captures de trames sur chaque segment IP du réseau.

1. Analyse de la table de mappage du routeur

L'administrateur utilise les commandes du routeur pour afficher la table de mappage NAT/PAT en cours sur l'interface 15.0.0.2.
Table de mappage NAT/PAT du routeur :

	Protocole	Ip privée	Port privé	Ip publique	Port public	Ip destination	Port destination
1	TCP	192.168.100.10	1414	15.0.0.2	1414	15.0.0.15	80
2	TCP	192.168.100.25	1414	15.0.0.2	1615	15.0.0.15	80

Questions :
1.1 Expliquer quel trafic réseau est à l'origine de ces lignes.
1.2 Donner l'adresse IP destination et le port destination utilisés par le serveur Web pour envoyer la page HTML demandée par le poste P2.
1.3 Expliquer pourquoi le port public de la ligne N°2 est différent du port privé.

2. La commande PING

L'administrateur lance de manière simultanée, à partir des postes **P1** et **P2**, la commande suivante :
PING 15.0.0.15

Il obtient sur les deux postes la réponse suivante :
Réponse de 15.0.0.15 : octets=32 temps=4 ms TTL=127

Les champs ICMP des premières trames capturées sont présentés en **Annexe 2**

Questions :
2.1 À quels échanges ICMP correspondent les trames 1, 3, 5 et 7 ?
2.2 À quels échanges ICMP correspondent les trames 2, 4, 6 et 8 ?
2.3 Justifier le changement de l'adresse IP source de la trame N°3 par rapport à la trame N°1.
2.4 Quel champ ICMP a été modifié par le routeur NAT/PAT pour distinguer les messages du poste **P1** avec ceux du poste **P2** ? Vérifier avec la description des messages donnée dans la RFC 792.

3. Autres trames capturées

Les captures présentent également les trames suivantes :

Trame 9
Adresse Ethernet destination 00 03 FF **40** 6C 35
Adresse Ethernet source 00 03 FF **42** 6C 35
Ip source : 192.168.100.25
Ip destination : 15.0.0.15
Champs ICMP (hexa) :

08	00	F2	5B
02	00	59	00
…	…	…	…

Trame 17
Adresse Ethernet destination 00 03 FF **40** 6C 35
Adresse Ethernet source 00 03 FF **42** 6C 35
Ip source : 192.168.100.25
Ip destination : 15.0.0.15
Champs ICMP (hexa) :

08	00	F1	5B
02	00	5A	00
…	…	…	…

Trame 25
Adresse Ethernet destination 00 03 FF **40** 6C 35
Adresse Ethernet source 00 03 FF **42** 6C 35
Ip source : 192.168.100.25
Ip destination : 15.0.0.15
Champs ICMP (hexa) :

08	00	F0	5B
02	00	5B	00
…	…	…	…

Questions
3.1 À quels messages ICMP correspondent les trames 9, 17 et 25 ?
3.2 En dehors du checksum, quel champ ICMP est modifié et pourquoi ?

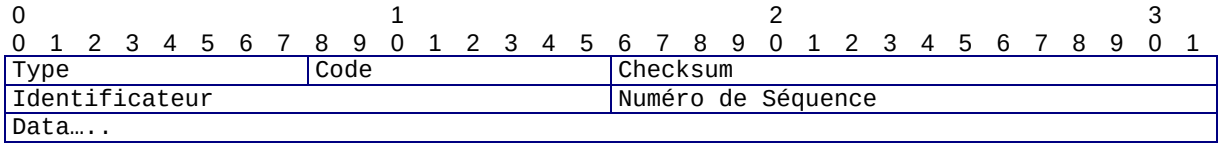
Annexes

Annexe 1 : 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

Introduction
Le Protocole Internet (IP) [1] est utilisé pour la transmission de datagrammes d'hôte à hôte à l'intérieur d'un système de réseaux interconnectés appelé Catenet [2]. Les appareils raccordant les réseaux entre eux sont appelés des Routeurs. Ces routeurs communiquent entre eux en utilisant le protocole Routeur à Routeur (GGP) [3,4] afin d'échanger des informations de contrôle et de gestion du réseau. Occasionnellement, un routeur ou un hôte destinataire peut avoir à communiquer vers l'émetteur du datagramme, par exemple, pour signaler une erreur de traitement du datagramme. C'est dans cette perspective qu'a été mis en place le protocole Internet Control Message Protocol (ICMP).
Il s'appuie sur le support de base fourni par IP comme s'il s'agissait d'un protocole d'une couche supérieure. ICMP n'en reste pas moins une partie intégrante du protocole IP, et doit de ce fait être implémenté dans chaque module IP.

Formats de message :

Message d'écho et de "réponse à écho"



Champs ICMP :

Type :	8 = écho; 0 = réponse à écho.
Code :	0
Checksum :	Le complément à un sur 16 bits de la somme des compléments à un du message ICMP. Lors du calcul du Checksum, le champ destiné à recevoir ce Checksum sera laissé à zéro. Si la longueur totale du message est un nombre impair d'octets, le calcul du Checksum se fera en ajoutant un dernier octet à zéro de bourrage en fin de message. Ce mécanisme de Checksum sera changé dans le futur.
Identificateur :	Si le code = 0, un identificateur permettant d'associer l'écho et la réponse à l'écho, peut être nul.
Numéro de séquence :	Si le code = 0, un numéro de séquence permettant d'associer l'écho et sa réponse. Peut être nul.

Description
Les données reçues dans un message d'écho doivent être réémises dans la réponse à l'écho. L'identificateur et le numéro de séquence peuvent être utilisés par l'émetteur du message d'écho afin d'associer facilement l'écho et sa réponse. Par exemple, l'identificateur peut être utilisé comme l'est un port pour TCP ou UDP, identifiant ainsi une session, et le numéro de séquence incrémenté pour chaque message d'écho envoyé. Le "miroir" respectera ces deux valeurs pour renvoyer le retour.
Les messages de code 0 peuvent provenir d'un routeur ou d'un hôte.

Références
[1] Postel, J. (ed.), "Internet Protocol - DARPA Internet Program Protocol Specification," RFC 791, USC/Information Sciences Institute, September 1981.
[2] Cerf, V., "The Catenet Model for Internetworking," IEN 48, Information Processing Techniques Office, Defense Advanced Research Projects Agency, July 1978.
[3] Strazisar, V., "Gateway Routing: An Implementation Specification", IEN 30, Bolt Beranek and Newman, April 1979.
[4] Strazisar, V., "How to Build a Gateway", IEN 109, Bolt Beranek and Newman, August 1979.

Annexe 2 : Champs ICMP des premières trames capturées lors de la commande PING

Trame 1
Adresse Ethernet destination 00 03 FF **40** 6C 35
Adresse Ethernet source 00 03 FF **42** 6C 35
Ip source : 192.168.100.25
Ip destination : 15.0.0.15
Champs ICMP (hexa) :

08	00	F3	5B
02	00	58	00
…	…	…	…

Trame 2
Adresse Ethernet destination 00 03 FF **40** 6C 35
Adresse Ethernet source 00 03 FF **41** 6C 35
Ip source : 192.168.100.10
Ip destination : 15.0.0.15
Champs ICMP (hexa) :

08	00	FC	5B
02	00	4F	00
…	…	…	…

Trame 3
Adresse Ethernet destination 00 03 FF **49** 6C 35
Adresse Ethernet source 00 03 FF **FD** FF FF
Ip source : 15.0.0.2
Ip destination : 15.0.0.15
Champs ICMP (hexa) :

08	00	F4	5B
01	00	58	00
…	…	…	…

Trame 4
Adresse Ethernet destination 00 03 FF **49** 6C 35
Adresse Ethernet source 00 03 FF **FD** FF FF
Ip source : 15.0.0.2
Ip destination : 15.0.0.15
Champs ICMP (hexa) :

08	00	FC	5B
02	00	4F	00
…	…	…	…

Trame 5
Adresse Ethernet destination 00 03 FF **FD** FF FF
Adresse Ethernet source 00 03 FF **49** 6C 35
Ip source : 15.0.0.15
Ip destination : 15.0.0.2
Champs ICMP (hexa) :

00	00	FC	5B
01	00	58	00
…	…	…	…

Trame 6
Adresse Ethernet destination 00 03 FF **FD** FF FF
Adresse Ethernet source 00 03 FF **49** 6C 35
Ip source : 15.0.0.15
Ip destination : 15.0.0.2
Champs ICMP (hexa) :

00	00	04	5C
02	00	4F	00
…	…	…	…

Trame 7
Adresse Ethernet destination 00 03 FF **42** 6C 35
Adresse Ethernet source 00 03 FF **40** 6C 35
Ip source : 15.0.0.15
Ip destination : 192.168.100.25
Champs ICMP (hexa) :

00	00	FB	5B
02	00	58	00
…	…	…	…

Trame 8
Adresse Ethernet destination 00 03 FF **41** 6C 35
Adresse Ethernet source 00 03 FF **40** 6C 35
Ip source : 15.0.0.15
Ip destination : 192.168.100.10
Champs ICMP (hexa) :

00	00	04	5C
02	00	4F	00
…	…	…	…