Travaux pratiques 6.7.2 : Examen des paquets ICMP

Schéma de topologie

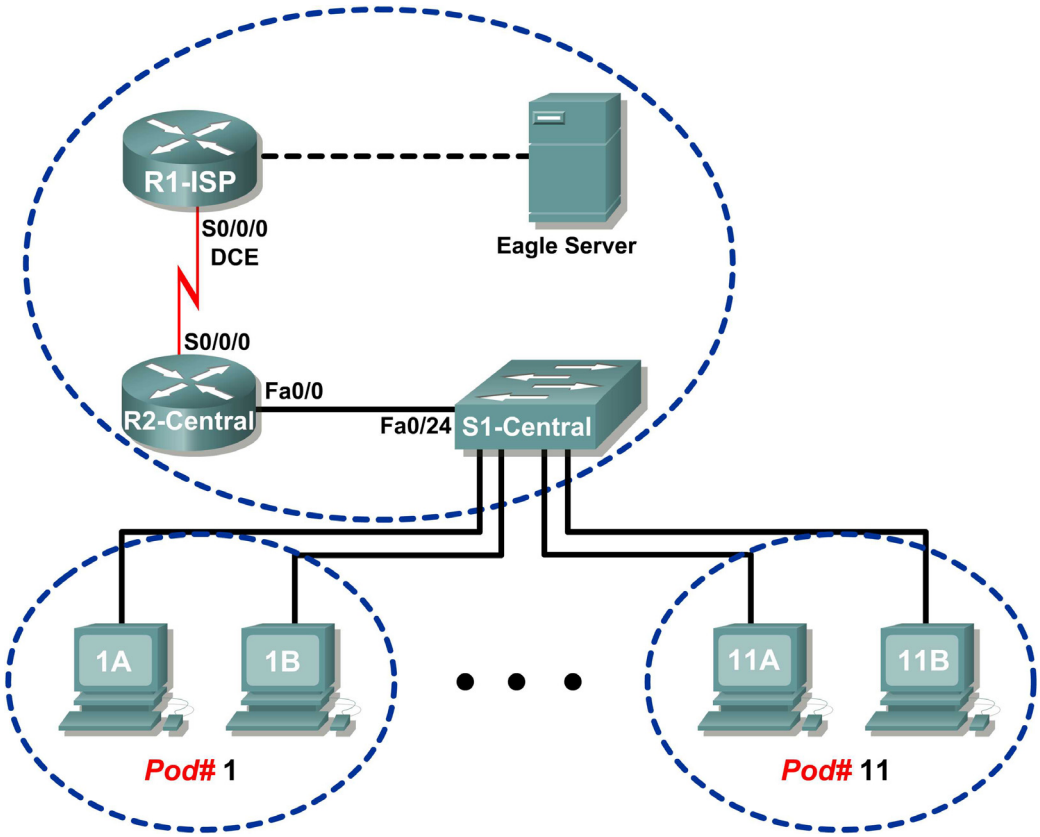


Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	S/O
	Fa0/0	192.168.254.253	255.255.255.0	S/O
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	S/O
	Fa0/0	172.16.255.254	255.255.0.0	S/O
Eagle Server	S/O	192.168.254.254	255.255.255.0	192.168.254.253
	S/O	172.31.24.254	255.255.255.0	S/O
host*Pod#*A	S/O	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#*B	S/O	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	S/O	172.16.254.1	255.255.0.0	172.16.255.254

Objectifs pédagogiques

À la fin de ce chapitre, vous saurez :

- comprendre le format des paquets ICMP ;
- utiliser Wireshark pour capturer et examiner les messages ICMP.

Contexte

Le protocole ICMP (Internet Control Message Protocol) a d'abord été défini dans la RFC 792, en septembre 1981. Les types de message ICMP ont été développés ultérieurement dans la RFC 1700. ICMP fonctionne sur la couche réseau TCP/IP et permet d'échanger les informations entre des périphériques.

Les paquets ICMP remplissent de nombreuses fonctions dans le réseau informatique actuel. Lorsqu'un routeur ne peut pas transmettre un paquet au réseau ou à l'hôte de destination, un message informatif est retourné à la source. En outre, les commandes **ping** et **tracert** envoient des messages ICMP aux destinations. Ensuite, ces dernières répondent avec des messages ICMP.

Scénario

À l'aide des travaux pratiques Eagle 1, les captures Wireshark se composent des paquets ICMP entre les périphériques réseau.

Tâche 1 : compréhension du format des paquets ICMP.

Paquet ICMP – Informations d'en-tête de message courantes

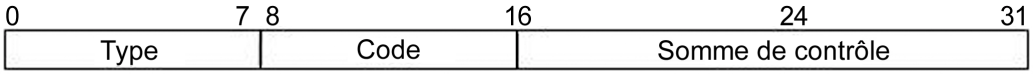


Figure 1. En-tête de message ICMP

Reportez-vous à la figure 1, les champs d'en-tête ICMP communs à tous les types de messages ICMP. Chaque message ICMP commence par un champ Type 8 bits, un champ Code 8 bits et une somme de contrôle 16 bits calculée. Le type de message ICMP décrit les champs ICMP restants. Le tableau dans la figure 2 illustre les types de message provenant de la RFC 792 :

Valeur	Signification
0	Réponse d'écho
3	Destination inaccessible
4	Épuisement de la source
5	Redirection
8	Écho
11	Dépassement du délai
12	Problème de paramètre
13	Horodatage
14	Réponse d'horodatage
15	Demande d'informations
16	Réponse à la demande d'informations

Figure 2. Types de message ICMP

Les codes offrent des informations complémentaires au champ Type. Par exemple, si le champ Type est 3, la destination inaccessible, d'autres informations sur le problème sont retournées dans le champ Code. Le tableau dans la figure 3 indique les codes pour le message Type 3 ICMP, la destination inaccessible, provenant de la RFC 1700 :

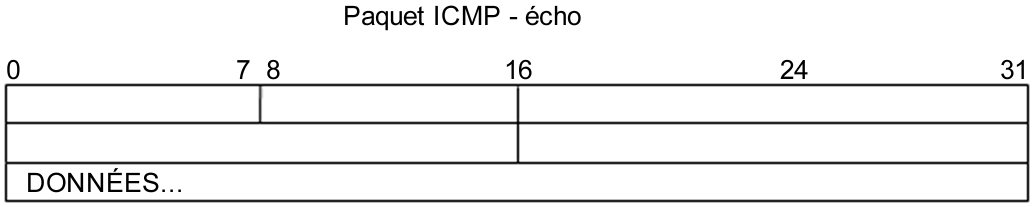
Code Valeur	Signification
0	Réseau inaccessible
1	Hôte inaccessible
2	Protocole inaccessible
3	Port inaccessible
4	Fragmentation requise et l'option Don't Fragment a été définie
5	Échec de la route source
6	Réseau de destination inconnu
7	Hôte de destination inconnu
8	Hôte source isolé
9	Communication avec réseau de destination interdit par l'administration
10	Communication avec hôte de destination Interdit par l'administration
11	Réseau de destination inaccessible pour le type de service
12	Hôte de destination inaccessible pour le type de service

Figure 3. Codes de messages type 3 ICMP

À l'aide de la capture de messages ICMP illustrée à la figure 4, renseignez les champs pour la requête d'écho des paquets ICMP. Les valeurs qui commencent par 0x sont des nombres hexadécimaux :

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x365c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

Figure 4. Requête d'écho des paquets ICMP

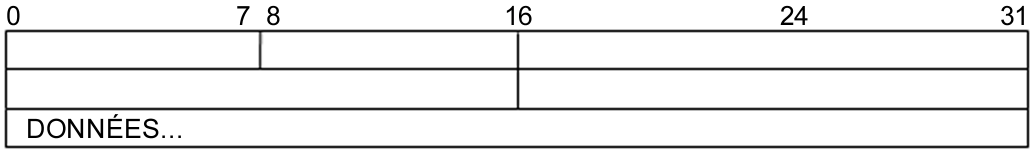


À l'aide de la capture de messages ICMP illustrée à la figure 5, renseignez les champs pour la réponse d'écho des paquets ICMP.

```
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x3e5c [correct]
  Identifier: 0x0200
  Sequence number: 0x1500
  Data (32 bytes)
```

Figure 5. Réponse d'écho des paquets ICMP

Paquet ICMP - écho



Sur la couche réseau TCP/IP, la communication entre les périphériques n'est pas garantie. Toutefois, ICMP n'offre pas de vérifications minimales pour qu'une réponse corresponde à la requête. À partir des informations disponibles dans les messages ICMP ci-dessus, comment l'expéditeur sait-il que la réponse s'applique à un écho spécifique ?

_____

_____

Tâche 2 : utilisation de Wireshark pour capturer et examiner les messages ICMP.

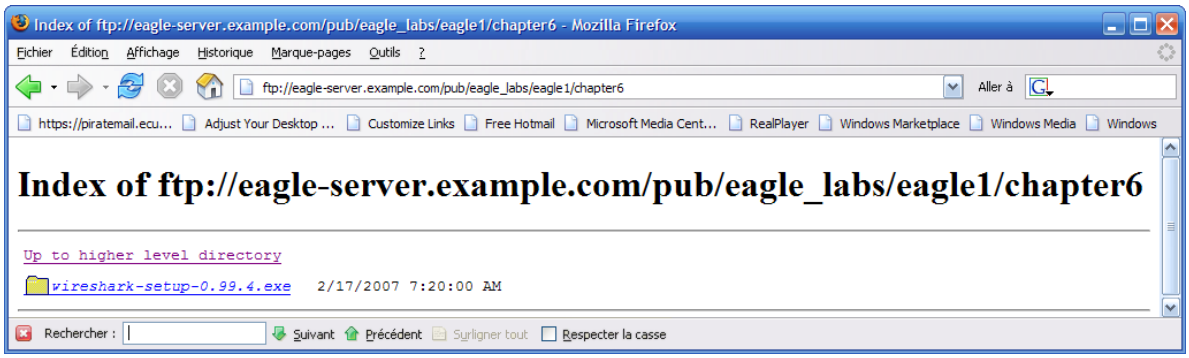


Figure 6. Site de téléchargement Wireshark

Si vous n'avez pas téléchargé Wireshark sur l'ordinateur hôte pod, il peut l'être à partir d'Eagle Server.

1. Ouvrez un navigateur Web, URL FTP://eagle-server.example.com/pub/eagle_labs/eagle1/chapter6, comme illustré à la figure 6.
2. Cliquez avec le bouton droit sur le nom de fichier de Wireshark, cliquez sur **Save Link As**, puis enregistrez le fichier dans l'ordinateur hôte pod.
3. Une fois le fichier téléchargé, ouvrez et installez Wireshark.

Étape 1 : capture et évaluation les messages d'écho ICMP vers Eagle Server.

Dans cette étape, Wireshark permet d'examiner les messages d'écho ICMP.

1. Ouvrez un terminal Windows sur l'ordinateur hôte pod.
2. Une fois prêt, démarrez la capture Wireshark.


```
C:\> ping eagle-server.example.com
Envoi d'une requête ping sur eagle-server.example.com [192.168.254.254]
avec 32 octets de données :
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=63
Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 7. Réponses `ping` validées depuis Eagle Server

3. À partir de la ligne de commande Windows, envoyez une requête **`ping`** à Eagle Server Quatre réponses validées doivent être reçues d'Eagle Server, comme illustré à la figure 7.
4. Arrêtez la capture Wireshark. Il doit y avoir un total de quatre requêtes d'écho ICMP et de réponses d'écho correspondantes, comme illustré à la figure 8.

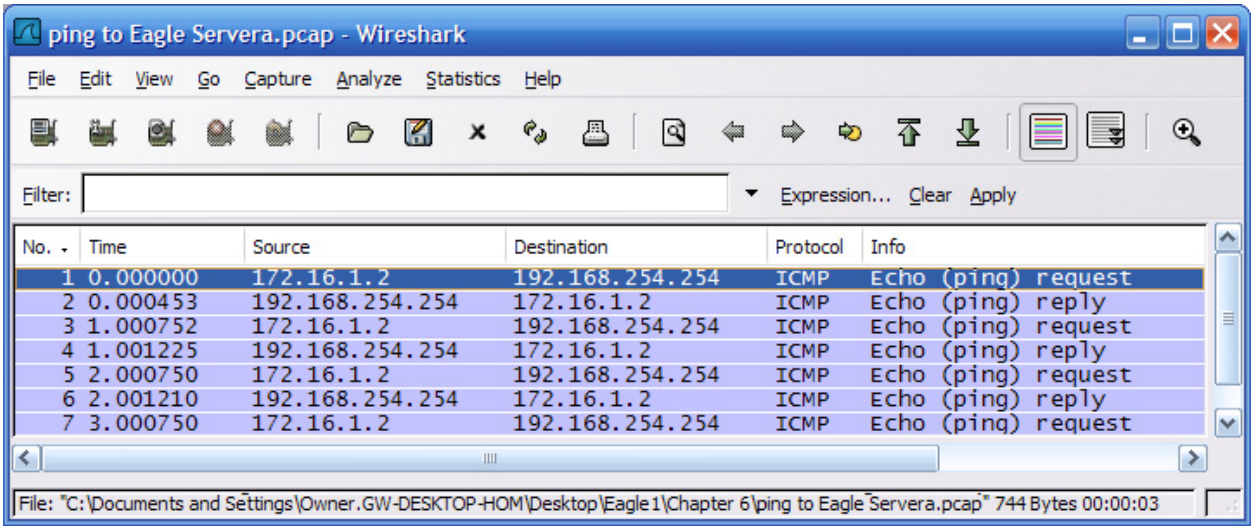


Figure 8. Capture Wireshark des requêtes et réponses `ping`

Quel périphérique réseau répond à la requête d'écho ICMP ? _____

5. Développez la fenêtre du milieu dans Wireshark, et l'enregistrement du protocole ICMP jusqu'à ce que tous les champs soient visibles. La fenêtre inférieure est également nécessaire à l'examen du champ Données.
6. Consignez les informations du *premier* paquet de requêtes d'écho vers Eagle Server :

Champ	Valeur
Type	
Code	
Somme de contrôle	
Identificateur	
Numéro d'ordre	
Données	

Y a-t-il 32 octets de données ? _____

7. Consignez les informations du *premier* paquet de réponses d'écho depuis Eagle Server :

Champ	Valeur
Type	
Code	
Somme de contrôle	
Identificateur	
Numéro d'ordre	
Données	

Quels champs, si c'est le cas, sont modifiés à partir de la requête d'écho ?

_____

8. Continuez d'évaluer les requêtes et réponses d'écho restantes. Renseignez les informations suivantes provenant de chaque nouveau ping :

Paquet	Somme de contrôle	Identificateur	Numéro d'ordre
Requête n°2			
Réponse n°2			
Requête n°3			
Réponse n°3			
Requête n°4			
Réponse n°4			

Pourquoi les valeurs de la somme de contrôle ont-elles changé avec chaque nouvelle requête ?

_____

Étape 2 : capture et évaluation des messages d'écho ICMP vers 192.168.253.1.

Dans cette étape, les requêtes ping sont envoyées vers un réseau et hôte fictifs. Les résultats de la capture Wireshark sont évalués, et sont parfois surprenants.

Essayez d'envoyer une requête à l'adresse IP 192.168.253.1.

```
C:\> ping 192.168.253.1
```

```
C:\> ping 192.168.253.1
Envoi d'une requête sur 192.168.253.1 avec 32 octets de données :
Réponse de 172.16.255.254 : Impossible de rejoindre l'hôte de
destination.
Réponse de 172.16.255.254 : Impossible de rejoindre l'hôte de
destination.
Réponse de 172.16.255.254 : Impossible de rejoindre l'hôte de
destination.
Réponse de 172.16.255.254 : Impossible de rejoindre l'hôte de
destination.
Statistiques Ping pour 192.168.253.1 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 9. Résultat du ping à partir d'une destination fictive

Reportez-vous à la figure 9. Au lieu d'un délai d'attente de la requête, une réponse d'écho a lieu.

Quel périphérique réseau répond à des requêtes ping vers une destination fictive ?

_____

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
2	0.000816	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
3	1.000854	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
4	1.001686	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
5	2.001815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
6	2.002547	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)
7	3.002815	172.16.1.2	192.168.253.1	ICMP	Echo (ping) request
8	3.003588	172.16.255.254	172.16.1.2	ICMP	Destination unreachable (Host unreachable)

Figure 10. Capture Wireshark à partir d'une destination fictive

Les captures Wireshark vers une destination fictive sont illustrées à la figure 10. Développez la fenêtre du milieu dans Wireshark, et l'enregistrement du protocole ICMP

Quel type de message ICMP permet de retourner les informations à l'expéditeur ?

_____

Quel est le code associé au type de message ?

_____

Étape 3 : capture et évaluation des messages d'écho ICMP qui dépassent la valeur TTL.

Dans cette étape, les requêtes ping sont envoyées avec une valeur TTL basse, et simule ainsi une destination inaccessible. Envoyez une requête ping à Eagle Server, et définissez la valeur TTL sur **1** :

```
C:\> ping -i 1 192.168.254.254
```

```
C:\> ping -i 1 192.168.254.254
Envoi d'une requête sur 192.168.254.254 avec 32 octets de données :
Réponse de 172.16.255.254 : Durée de vie expirée lors du transit.
Réponse de 172.16.255.254 : Durée de vie expirée lors du transit.
Réponse de 172.16.255.254 : Durée de vie expirée lors du transit.
Réponse de 172.16.255.254 : Durée de vie expirée lors du transit.
Statistiques Ping pour 192.168.254.254 :
    Paquets : Envoyés = 4, Reçus = 4, Perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0 ms, Maximum = 0 ms, Moyenne = 0 ms
C:\>
```

Figure 11. Résultats du ping pour une valeur TTL dépassée

Reportez-vous à la figure 11, qui indique les réponses ping lors du dépassement de la valeur TTL.

Quel périphérique réseau répond aux requêtes ping qui dépassent la valeur TTL ?

_____

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
2	0.000701	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
3	1.000003	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
4	1.000687	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
5	1.999996	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
6	2.000761	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)
7	3.000970	172.16.1.2	192.168.254.254	ICMP	Echo (ping) request
8	3.001723	172.16.255.254	172.16.1.2	ICMP	Time-to-live exceeded (Time to live exceeded in transit)

Figure 12. Capture Wireshark d'une valeur TTL dépassée

Les captures Wireshark vers une destination fictive sont illustrées à la figure 12. Développez la fenêtre du milieu dans Wireshark, et l'enregistrement du protocole ICMP.

Quel type de message ICMP permet de retourner les informations à l'expéditeur ?

_____

Quel est le code associé au type de message ?

_____

Quel périphérique réseau est responsable de la décrémentation de la valeur TTL ?

_____

Tâche 3 : confirmation

Utilisez Wireshark pour capturer une session **`tracert`** vers Eagle Server, puis vers 192.168.254.251. Examinez le message de la valeur TTL dépassée pour ICMP. Ceci montre la manière dont la commande **`tracert`** suit le chemin du réseau vers la destination.

Tâche 4 : remarques générales

Le protocole ICMP est très utile lors du dépannage de problèmes de connectivité réseau. Sans messages ICMP, un expéditeur est dans l'incapacité d'expliquer l'échec de la connexion de la destination. À l'aide de la commande **`ping`**, différentes valeurs de types de message ICMP ont été capturées et évaluées.

Tâche 5 : nettoyage

Il se peut que Wireshark ait été chargé sur l'ordinateur hôte pod. Si le programme doit être supprimé, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**, puis faites défiler la liste vers le bas jusqu'à Wireshark. Cliquez sur le nom de fichier, sur **Supprimer**, puis suivez les instructions de désinstallation.

Supprimez tout fichier pcap de Wireshark qui a été créé sur l'ordinateur hôte pod.

Sauf indication contraire du formateur, mettez les ordinateurs hôtes hors tension. Enlevez le matériel utilisé durant les travaux pratiques, et préparez la salle pour le cours suivant.

