Travaux pratiques 7.5.2 : Examen des trames

Schéma de topologie

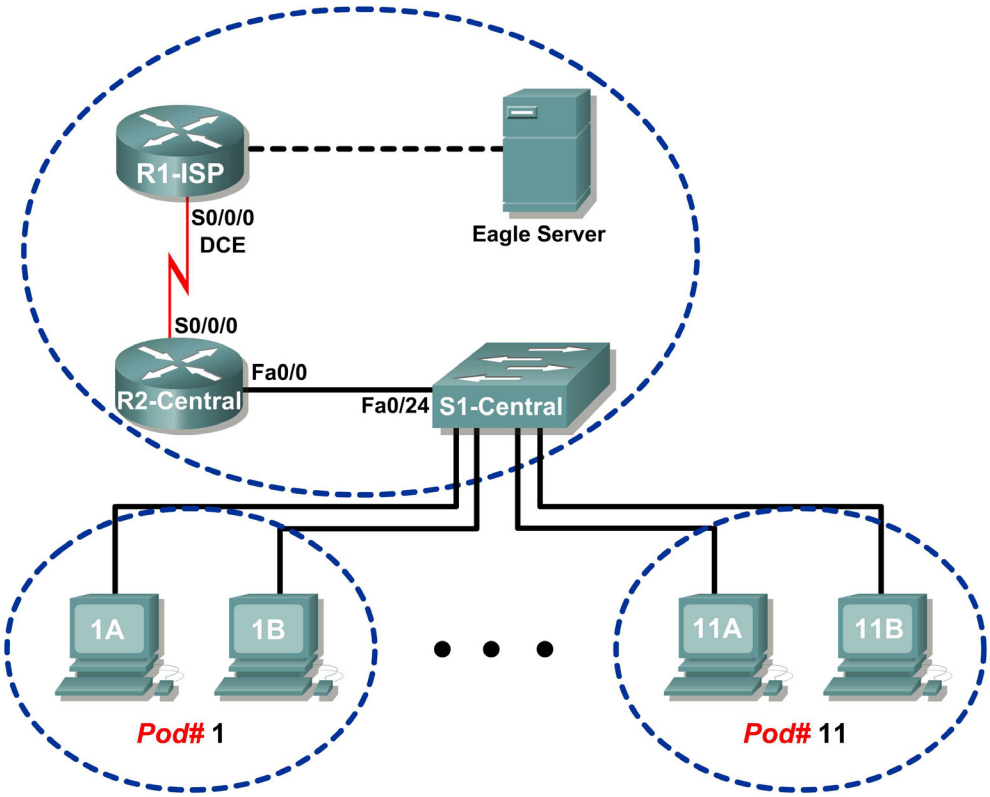

Table d'adressage

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 :

- expliquer les champs d'en-tête dans une trame Ethernet II ;
- utiliser Wireshark pour capturer et analyser les trames Ethernet II.

Contexte

Lorsque des protocoles de couche supérieure communiquent entre eux, les données circulent dans les couches du modèle OSI et sont encapsulées dans une trame de couche 2. La composition des trames dépend du type d'accès aux supports. Par exemple, si le protocole de couche supérieure est TCP/IP et que l'accès aux supports est Ethernet, l'encapsulation des trames de couche 2 est Ethernet II.

Lorsque vous étudiez les concepts de couche 2, il est utile d'analyser les informations d'en-tête des trames. L'en-tête de trame Ethernet II est examiné dans ces travaux pratiques. Les trames Ethernet II peuvent prendre en charge différents protocoles de couche supérieure, tels que TCP/IP.

Scénario

Wireshark permet de capturer et d'analyser les champs d'en-tête de trames Ethernet II. Si vous n'avez pas effectué le téléchargement de Wireshark sur l'ordinateur hôte pod, utilisez l'adresse URL `ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter7/`, fichier `wireshark-setup-0.99.4.exe`.

La commande **`ping`** de Windows permet de générer le trafic réseau pour la capture Wireshark.

Tâche 1 : expliquer les champs d'en-tête dans une trame Ethernet II.

Le format d'une trame Ethernet II est illustré à la figure 1.

Structure de trame Ethernet II

Préambule	Adresse de destination	Adresse source	Type de trame	Données	FCS
8 Octets	6 Octets	6 Octets	2 Octets	46- 1500 Octets	4 Octets

Figure 1. Format de trame Ethernet II

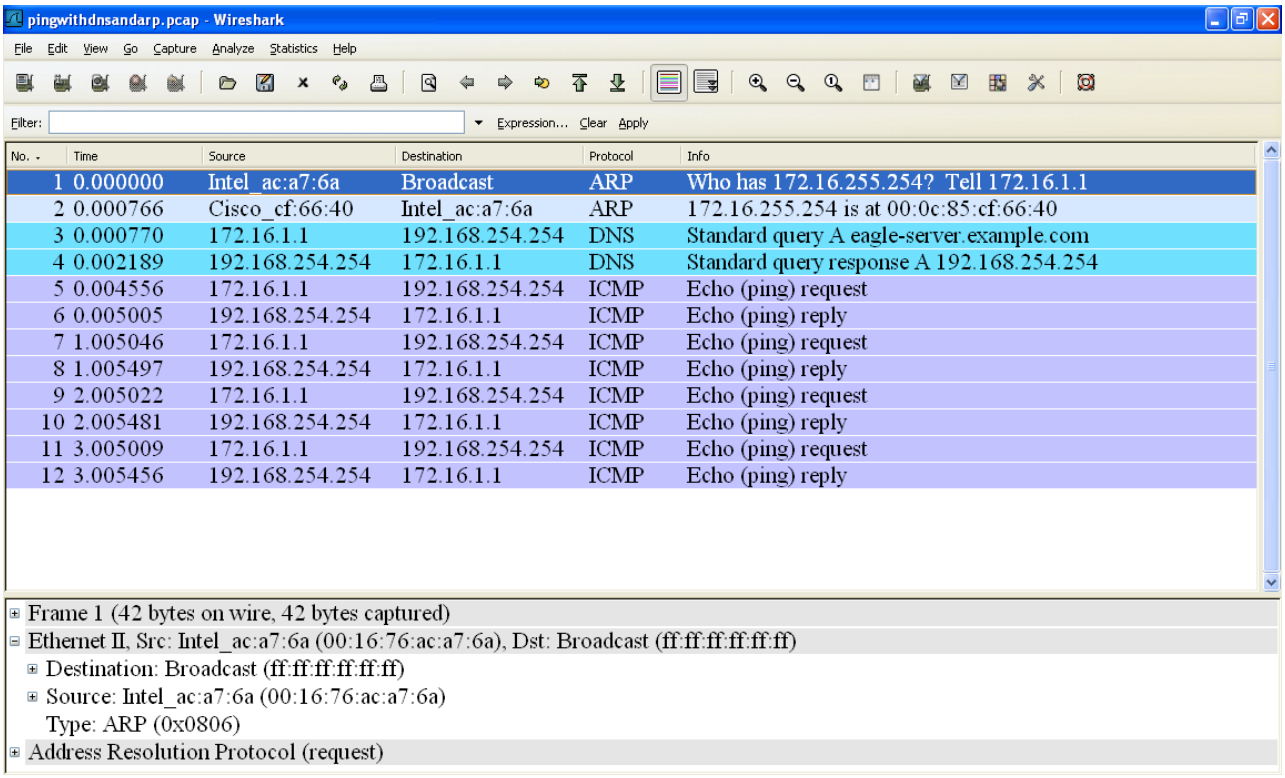

Figure 2. Capture Wireshark de la commande `ping`

À la figure 2, la fenêtre Panel List affiche une capture Wireshark d'une commande **`ping`** entre un ordinateur hôte pod et Eagle Server. La session commence par le protocole qui recherche l'adresse MAC du routeur de passerelle, suivi d'une demande DNS. Finalement, la commande **`ping`** exécute des requêtes d'écho.

À la figure 2, la fenêtre Packet Details affiche les informations détaillées de la trame 1. À l'aide de cette fenêtre, il est possible d'obtenir les informations suivantes sur la trame Ethernet II :

Champ	Valeur	Description
Préambule	Non affichée dans la capture.	Ce champ contient des bits de synchronisation traités par la carte réseau.
Adresse de destination	`ff:ff:ff:ff:ff:ff`	Les adresses de couche 2 pour la trame. La longueur de chaque adresse est de 48 bits, ou 6 octets, exprimés en 12 chiffres hexadécimaux, `0-9,A-F`. Le format courant est le suivant : `12:34:56:78:9A:BC`. Les six premiers numéros hexadécimaux indiquent le fabricant de la carte réseau (NIC). Reportez-vous à http://www.neotechcc.org/forum/macid.htm pour obtenir une liste de codes fournisseurs. Les six derniers chiffres hexadécimaux, `ac:a7:6a`, ont le numéro de série de la carte réseau. L'adresse de destination peut être une adresse de diffusion qui ne contient que des `1` ou à monodiffusion. L'adresse source est toujours à monodiffusion.
Adresse source	`00:16:76:ac:a7:6a`	

Champ	Valeur	Description
Type de trame	0x0806	Pour les trames Ethernet II, ce champ contient une valeur hexadécimale qui permet d'indiquer le protocole de couche supérieure dans le champ de données. De nombreux protocoles de couche supérieure sont pris en charge par Ethernet II. Deux types de trame standard sont : Valeur Description 0x0800 Protocole IPv4 0x0806 Résolution de l'adresse ARP
Données	ARP	Contient le protocole encapsulé de niveau supérieur. Le champ de données comprend entre 46 et 1500 octets.
FCS	Non affichée dans la capture.	Séquence de contrôle de trame, que la carte réseau utilise pour identifier les erreurs au cours de la transmission. La valeur est calculée par l'ordinateur émetteur, et englobe les adresses de trames, le type et le champ de données. Elle est vérifiée par le récepteur.

Quelle est la signification de tous les **1** dans le champ adresse de destination ?

_____

_____

À partir des informations contenues dans la fenêtre Packet List pour la **première** trame, répondez aux questions suivantes sur les adresses MAC source et de destination.

Adresse de destination :

Adresse MAC : _____
Fabricant de la carte réseau : _____
Numéro de série de la carte réseau : _____

Adresse source :

Adresse MAC : _____
Fabricant de la carte réseau : _____
Numéro de série de la carte réseau : _____

À partir des informations contenues dans la fenêtre Packet List pour la **deuxième** trame, répondez aux questions suivantes sur les adresses MAC source et de destination.

Adresse de destination :

Adresse MAC : _____
Fabricant de la carte réseau : _____
Numéro de série de la carte réseau : _____

Adresse source :

Adresse MAC : _____
Fabricant de la carte réseau : _____
Numéro de série de la carte réseau : _____

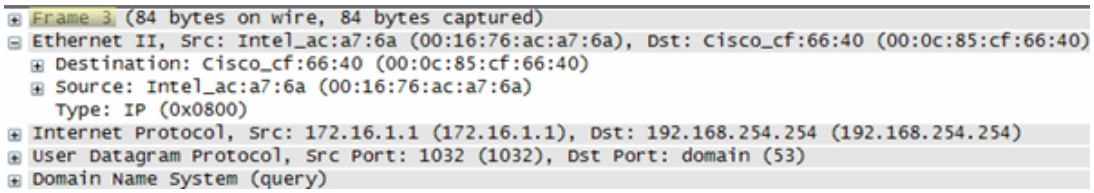

Figure 3. Champs de trame 3

La figure 3 contient une vue éclatée de la capture Wireshark de trame 3. Utilisez ces informations pour remplir le tableau suivant :

Champ	Valeur
Préambule	
Adresse de destination	
Adresse source	
Type de trame	
Données	
FCS	

Dans la tâche suivante, Wireshark permet de capturer et d'analyser des paquets capturés sur l'ordinateur hôte pod.

Tâche 2 : utilisation de Wireshark pour capturer et analyser les trames Ethernet II.

Étape 1 : configuration de Wireshark pour les captures de paquets.

Préparez Wireshark pour les captures. Cliquez sur **Capture > Interfaces**, puis cliquez sur le bouton Démarrer qui correspond à l'adresse IP de l'interface 172.16.x.y. Ceci permet de commencer la capture des paquets.

Étape 2 : démarrage d'une requête ping vers Eagle Server et capture de la session.

Ouvrez une fenêtre de terminal Windows. Cliquez sur **Démarrer > Exécuter**, tapez **cmd**, puis cliquez sur **OK**.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62
Réponse de 192.168.254.254 : octets=32 temps<1 ms TTL=62

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 4. Ping vers eagle-server.example.com

Envoyez une requête ping vers eagle-server.example.com, comme illustré à la figure 4. Lorsque la commande a terminé l'exécution, arrêtez les captures Wireshark.

Étape 3 : analyse de la capture Wireshark.

La fenêtre Packet List de Wireshark démarre avec une requête et une réponse ARP pour l'adresse MAC de la passerelle. Ensuite, une requête DNS est effectuée pour l'adresse IP de eagle-server.example.com. Finalement, la commande **ping** est exécutée. Votre capture doit être semblable à celle illustrée à la figure 2.

Utilisez votre capture Wireshark de la commande **ping** pour répondre aux questions suivantes :

Informations sur l'adresse MAC de l'ordinateur pod :

Adresse MAC : _____
Fabricant de la carte réseau : _____
Numéro de série de la carte réseau : _____

Informations sur l'adresse MAC de R2-Central :

Adresse MAC : _____
Fabricant de la carte réseau : _____
Numéro de série de la carte réseau : _____

Un participant d'un autre établissement souhaite connaître l'adresse MAC d'Eagle Server. Que lui diriez-vous ?

Quelle est la valeur du type de trame Ethernet II pour une requête ARP ? _____

Quelle est la valeur du type de trame Ethernet II pour une réponse ARP ? _____

Quelle est la valeur du type de trame Ethernet II pour une requête DNS ? _____

Quelle est la valeur du type de trame Ethernet II pour une réponse de requête DNS ?
_____

Quelle est la valeur du type de trame Ethernet II pour un écho ICMP ? _____

Quelle est la valeur du type de trame Ethernet II pour une réponse d'écho ICMP ?
_____

Tâche 3 : confirmation

Wireshark permet de capturer des sessions provenant d'autres protocoles TCP/IP, tels que FTP et HTTP. Analysez les paquets capturés et vérifiez que le type de trame Ethernet II reste `0x0800`.

Tâche 4 : remarques générales

Dans ces travaux pratiques, les informations d'en-tête de trames Ethernet II ont été examinées. Un champ préambule contient sept octets de séquences `0101` alternatives, et un octet qui signale le début de la trame, `01010110`. Les adresses MAC source et de destination contiennent 12 chiffres hexadécimaux. Les six premiers chiffres hexadécimaux contiennent le fabricant de la carte réseau, et les six derniers chiffres hexadécimaux contiennent le numéro de série de la carte réseau. Si la trame est une diffusion, l'adresse MAC de destination ne contient que des `1`. Un champ type de trame à 4 octets contient une valeur qui indique le protocole dans le champ de données. Pour IPv4, la valeur est `0x0800`. Le champ de données est variable et contient le protocole encapsulé de la couche supérieure. À la fin de la trame, une valeur FCS de 4 octets permet de vérifier l'absence d'erreurs lors de la transmission.

Tâche 5 : nettoyage

Wireshark a été installé sur l'ordinateur hôte pod. Si Wireshark doit être désinstallé, cliquez sur **Démarrer > Panneau de configuration**. Ouvrez **Ajout/Suppression de programmes**. Sélectionnez Wireshark, puis cliquez sur **Supprimer**.

Supprimez tout fichier créé sur l'ordinateur hôte pod au cours des travaux pratiques.

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.

