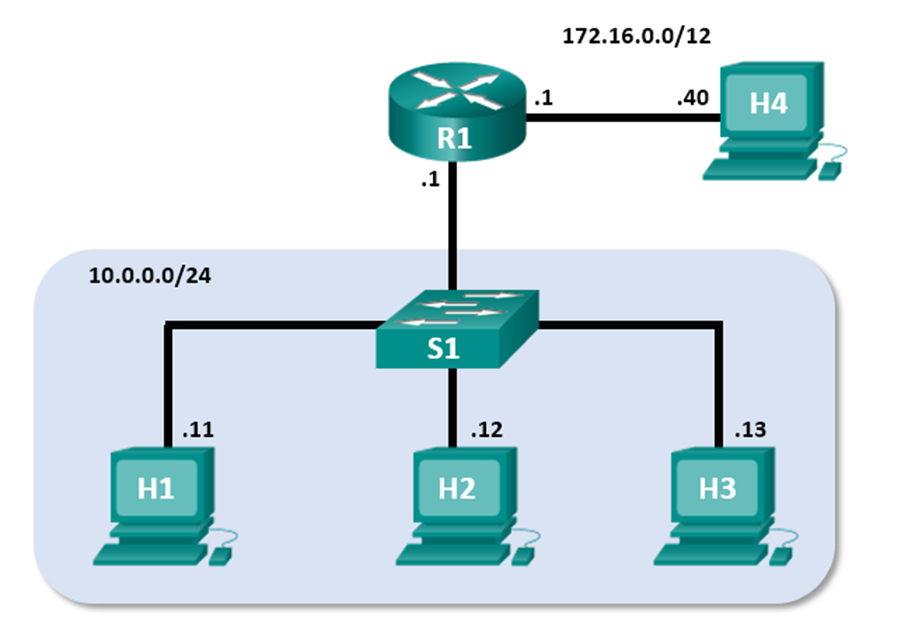
Travaux pratiques - Utilisation de Wireshark pour examiner les trames Ethernet

Topologie de Mininet



# Objectifs

Partie 1 : examiner les champs d'en-tête dans une trame Ethernet II

Partie 2 : utiliser Wireshark pour capturer et analyser les trames Ethernet

# Contexte/scénario

Lorsque des protocoles de couche supérieure communiquent entre eux, les données circulent dans les couches du modèle OSI (Open Systems Interconnection) et sont encapsulées dans une trame de couche 2. La composition des trames dépend du type d'accès aux supports. Par exemple, si les protocoles de couche supérieure sont TCP et IP et que l'accès aux supports est Ethernet, l'encapsulation des trames de couche 2 est Ethernet II. C'est généralement le cas pour un environnement de réseau local (LAN).

Lorsque vous étudiez les concepts de couche 2, il est utile d'analyser les informations d'en-tête des trames. Dans la première partie de ce TP, vous allez examiner les champs figurant dans une trame Ethernet II. Dans la deuxième partie, vous allez utiliser Wireshark pour capturer et analyser les champs d'en-tête de trame Ethernet II pour le trafic local et distant.

# Ressources requises

* Poste de travail CyberOps VM

# Instructions

## Examiner les champs d'en-tête dans une trame Ethernet II

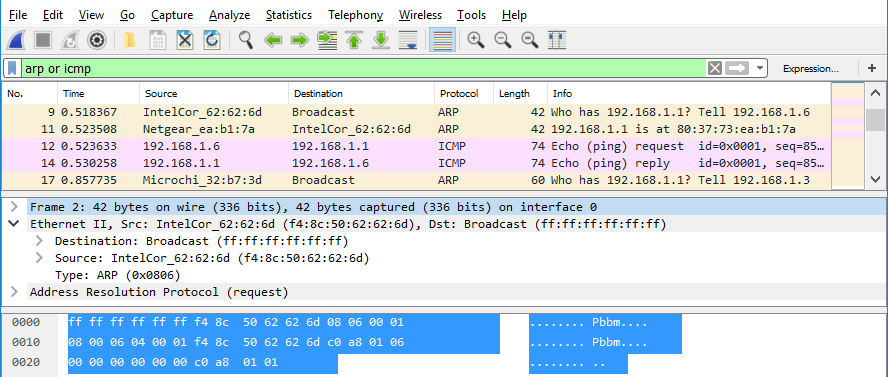
Dans la première partie, vous allez examiner les champs d'en-tête et le contenu d'une trame Ethernet II qui vous est fournie. Une capture Wireshark sera utilisée pour examiner le contenu de ces champs.

### Consultez les descriptions et les longueurs des champs d'en-tête Ethernet II.

| Préambule | Adresse de  destination | Adresse  source | Type de trame | Données | FCS |
| --- | --- | --- | --- | --- | --- |
| 8 octets | 6 octets | 6 octets | 2 octets | De 46 à 1 500 octets | 4 octets |

### Examinez les trames Ethernet dans une capture Wireshark.

La capture Wireshark ci-dessous illustre les paquets générés par une requête ping envoyée depuis un ordinateur hôte à sa passerelle par défaut. Un filtre a été appliqué à Wireshark pour afficher les protocoles ARP et ICMP uniquement. La session commence par une requête ARP pour l'adresse MAC du routeur de passerelle, suivie de quatre requêtes ping et réponses.



### Examinez le contenu d'en-tête Ethernet II d'une requête ARP.

Le tableau suivant prend la première trame dans la capture Wireshark et affiche les données présentes dans les champs d'en-tête 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  Adresse source | Diffusion (ff:ff:ff:ff:ff:ff)  IntelCor\_62:62:6d  (f4:8c:50:62:62:6d) | 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, de 0 à 9 et de A à F. Le format suivant est courant : 12:34:56:78:9A:BC.  Les six premiers chiffres hexadécimaux indiquent le fabricant de la carte réseau, les six derniers chiffres hexadécimaux correspondent au numéro de série de la carte réseau.  L'adresse de destination peut être une adresse de diffusion, qui ne contient que des 1, ou une adresse de monodiffusion. L'adresse source est toujours à monodiffusion. |
| Type de trame | 0x0806 | Pour les trames Ethernet II, ce champ contient une valeur hexadécimale qui permet d'indiquer le type de 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 IPv4 Protocol  0x0806 Protocole ARP (Address Resolution Protocol) |
| Données | ARP | Contient le protocole encapsulé de niveau supérieur. Le champ de données comprend entre 46 et 1 500 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. |

#### Questions :

Quel élément est important en ce qui concerne le contenu du champ d'adresse de destination ?

L’élément qui est important en ce qui concerne le contenu du champ d’adresse de destination est l’adresse MAC de la machine dont on souhaite connaitre l’adresse IP.

Pourquoi l'ordinateur envoie-t-il une diffusion ARP avant d'envoyer la première requête ping ?

L'objectif de la diffusion ARP est de demander à la machine qui possède l'adresse IP spécifiée de répondre avec son adresse MAC. Ainsi, l'ordinateur qui a envoyé la diffusion ARP pourra connaître l'adresse MAC de la machine destinataire et pourra ensuite établir une communication directe.

Quelle est l'adresse MAC de la source dans la première trame ?

L’adresse MAC de la source dans la première trame est : f4 8c 50 62 62 6d.

Elle est composée en deux parties :

* f4 8c 50 : Indique fabricant de la carte réseau.
* 62 62 6d : Indique le numéro de série de la carte réseau.

Quel est l'ID du fournisseur (OUI) de la carte réseau source ?

L’ID du fournisseur de la carte réseau source sont les 3 premiers octets de l’adresse MAC :

* f4 8c 50

À quelle partie de l'adresse MAC correspond l'identifiant OUI ?

La partie de l’adresse MAC qui correspond à l’identifiant sont les 3 derniers octets de l’adresse MAC :

* 62 62 6d

Quel est le numéro de série de la carte réseau source ?

D’après l’adresse MAC, nous savons que l’identifiant de la carte réseau est 62 62 6d. Cependant, nous ne pouvons pas connaitre le numéro de série de la carte réseau source car cette donnée est une donnée interne au fabriquant et n’est donc pas encapsulé dans l’adresse MAC.

## Utiliser Wireshark pour capturer et analyser les trames Ethernet

Dans la deuxième partie, vous allez utiliser Wireshark pour capturer les trames Ethernet locales et distantes. Vous examinerez ensuite les informations contenues dans les champs d'en-tête de trame.

### Étudiez la configuration réseau de H3.

* + - 1. Démarrez et connectez-vous à votre poste de travail CyberOps VM avec les informations d'identification suivantes:

Nom d'utilisateur : **analyst** Mot de passe : **cyberops**

* + - 1. Ouvrez un émulateur de terminal pour lancer mininet et saisissez la commande suivante à l'invite. Lorsque le système vous y invite, saisissez le mot de passe **cyberops**.

[analyst@secOps ~]$ **sudo ./lab.support.files/scripts/cyberops\_topo.py**

[sudo] password for analyst:

* + - 1. À l'invite de mininet, démarrez les fenêtres de terminal sur l'hôte H3.

\*\*\* À partir de l'interface de ligne de commande :

mininet> **xterm H3**

* + - 1. À l'invite Node: h3, saisissez **ip address** pour vérifier l'adresse IPv4 et enregistrez l'adresse MAC.

|  |  |  |
| --- | --- | --- |
| Host-interface | Adresse IP | Adresse MAC |
| H3-eth0 |  |  |

* + - 1. À l'invite de Node : H3, saisissez **netstat -r** pour afficher les informations de passerelle par défaut.

[root@secOps ~]# **netstat -r**

Table de routage IP du noyau

Destination Gateway Genmask Flags MSS Window irtt Iface

default 10.0.0.1 0.0.0.0 UG 0 0 0 H3-eth0

10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 H3-eth0

#### Question :

Quelle est l'adresse IP de la passerelle par défaut pour l'hôte H3 ?

L’adresse IP de la passerelle par défaut pour l’hôte H3 est : 10.0.0.1

### Videz le cache ARP cache sur H3 et commencez à capturer le trafic sur H3-eth0.

* + - 1. Dans la fenêtre de terminal de Node : H3, saisissez **arp - n** pour afficher le contenu du cache ARP.

[root@secOps analyst]# **arp -n**

* + - 1. S'il existe des informations ARP dans le cache, videz-le via la commande suivante : **arp -d *IP-address***. Répétez cette opération jusqu'à ce que toutes les informations mises en cache aient été effacées.

[root@secOps analyst]# **arp -n**

Address HWtype HWaddress Flags Mask Iface

10.0.0.11 ether 5a:d0:1d:01:9f:be C H3-eth0

[root@secOps analyst]# **arp -d 10.0.0.11**

Address HWtype HWaddress Flags Mask Iface

10.0.0.11 (incomplete) C H3-eth0

* + - 1. Dans la fenêtre de terminal de Node : H3, ouvrez Wireshark et lancez une capture de paquets pour l'interface eth0-H3.

[root@secOps analyst]# **wireshark-gtk &**

### Envoyez une requête ping H1 depuis H3.

* + - 1. Depuis le terminal sur H3, envoyez une requête ping à la passerelle par défaut et arrêtez après l'envoi de 5 paquets de requêtes d'écho.

[root@secOps analyst]# **ping -c 5 10.0.0.1**

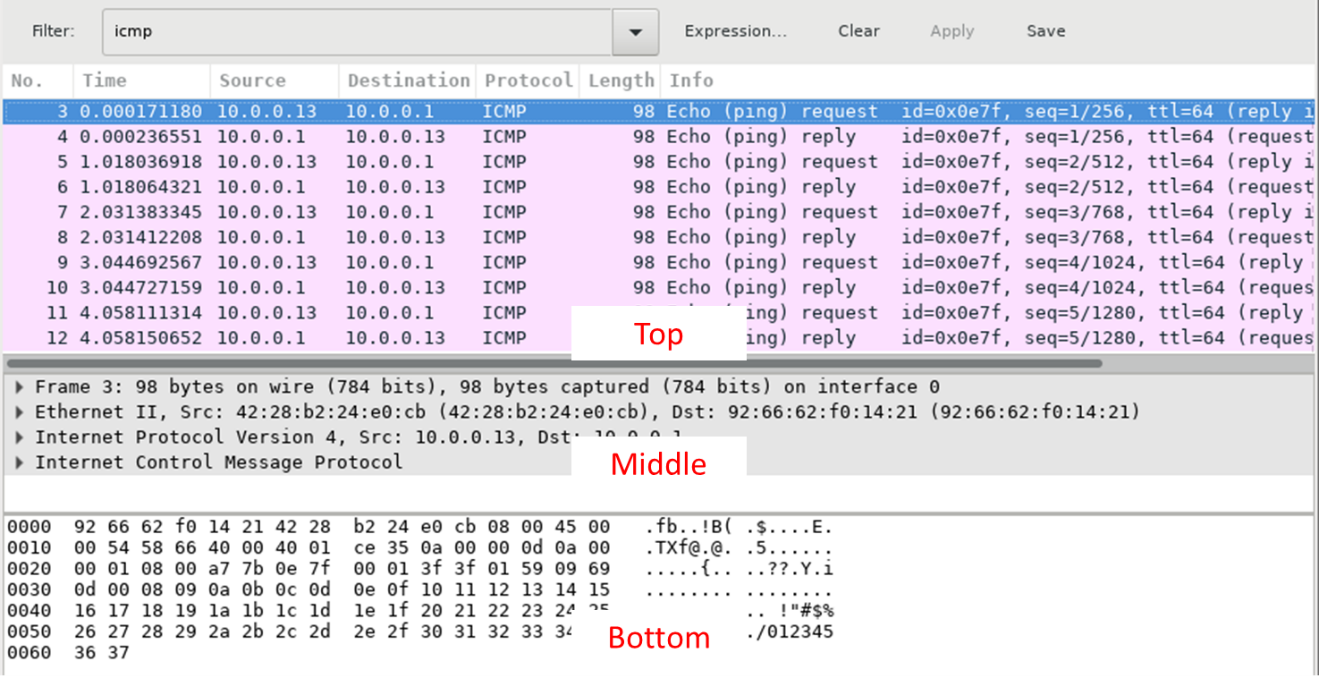
* + - 1. Une fois la requête ping terminée, arrêtez la capture Wireshark.

### Filtrez Wireshark pour afficher uniquement le trafic ICMP.

Appliquez le filtre **icmp** au trafic capturé pour que le trafic ICMP apparaisse dans les résultats.

### Examinez la première requête Echo (ping) dans Wireshark.

La fenêtre principale de Wireshark est divisée en trois sections : le volet Packet List (liste des paquets, en haut), le volet Packet Details (détails des paquets, au milieu) et le volet Packet Bytes (octets des paquets, en bas). Si vous avez sélectionné l'interface appropriée pour la capture des paquets à l'étape 3, Wireshark doit afficher les informations ICMP dans le volet Packet List de Wireshark, comme dans l'exemple suivant.



* + - 1. Dans le volet Packet List (section supérieure), cliquez sur la première trame répertoriée. **Echo (ping) request** (requête écho (ping)) devrait s'afficher en dessous de l'en-tête **Info**. La ligne devrait également être surlignée en bleu.
      2. Examinez la première ligne du volet Packet Details (section centrale). Cette ligne indique la longueur de la trame : 98 octets dans cet exemple.
      3. La deuxième ligne dans le volet Packet Details indique qu'il s'agit d'une trame Ethernet II. Les adresses MAC source et de destination sont également indiquées.

#### Questions :

Quelle est l'adresse MAC de la carte réseau de l'ordinateur ?

Quelle est l'adresse MAC de la passerelle par défaut ?

* + - 1. Vous pouvez cliquer sur la flèche au début de la deuxième ligne afin d'obtenir des informations supplémentaires sur la trame Ethernet II.

#### Question :

Quel type de trame est affiché ?

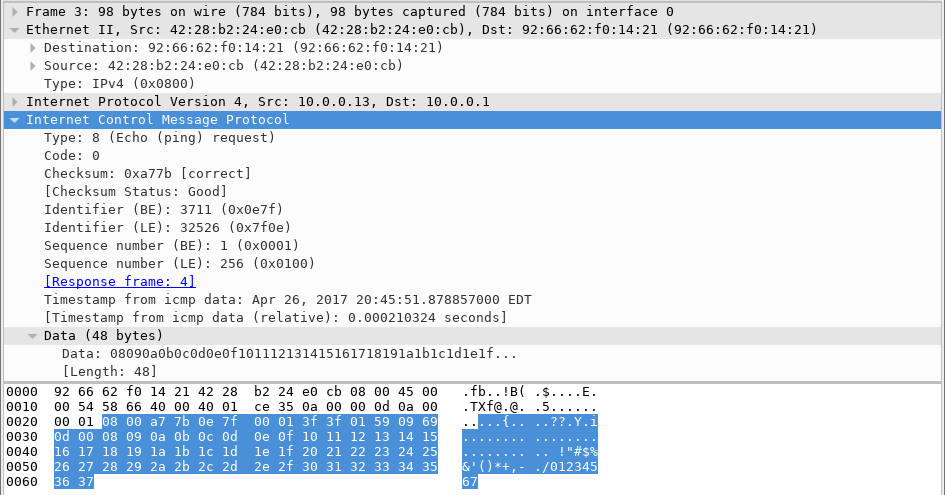
* + - 1. Les deux dernières lignes figurant dans la section centrale fournissent des informations sur le champ de données de la trame. Notez que les données contiennent les informations d'adresse IPv4 de la source et de la destination.

#### Questions :

Quelle est l'adresse IP source ?

Quelle est l'adresse IP de destination ?

* + - 1. Vous pouvez cliquer sur n'importe quelle ligne dans la section centrale pour mettre en surbrillance cette partie de la trame (hex et ASCII) dans le volet Packet Bytes (section inférieure). Cliquez sur la ligne **Internet Control Message Protocol** (protocole ICMP) dans la section centrale et examinez ce qui est mis en surbrillance dans le volet Packet Bytes.



* + - 1. Cliquez sur la trame suivante dans la section supérieure et examinez une trame de réponse Echo. Notez que les adresses MAC source et de destination ont été inversées, car cette trame a été envoyée depuis le routeur de passerelle par défaut comme réponse au premier ping.

#### Question :

Quel périphérique et quelle adresse MAC s'affichent comme adresse de destination ?

### Lancez une nouvelle capture dans Wireshark.

* + - 1. Cliquez sur l'icône **Start Capture** (démarrer la capture) pour démarrer une nouvelle capture Wireshark. Une fenêtre contextuelle vous invite à enregistrer les précédents paquets capturés dans un fichier avant de démarrer une nouvelle capture. Cliquez sur **Continue without Saving** (continuer sans enregistrer).
      2. Dans la fenêtre du terminal de Node : H3, envoyez 5 paquets de requêtes d'écho à 172.16.0.40.
      3. Arrêtez la capture des paquets une fois les requêtes ping terminées.

### Examinez les nouvelles données dans le volet de la liste des paquets de Wireshark.

#### Questions :

Dans la première trame de demande Echo (ping), quelles sont les adresses MAC source et de destination ?

**Source**:

**Destination**:

Saisissez vos réponses ici

Quelles sont les adresses IP source et de destination figurant dans le champ de données de la trame ?

**Source**:

**Destination**:

Comparez ces adresses à celles que vous avez reçues à l'étape 5. La seule adresse qui a changé est l'adresse IP de destination.

#### Question :

Pourquoi l'adresse IP de destination a-t-elle changé, alors que l'adresse MAC de destination est restée la même ?

# Remarques générales

Wireshark n'affiche pas le champ de préambule d'un en-tête de trame. Que contient le champ de préambule ?

Fin du document