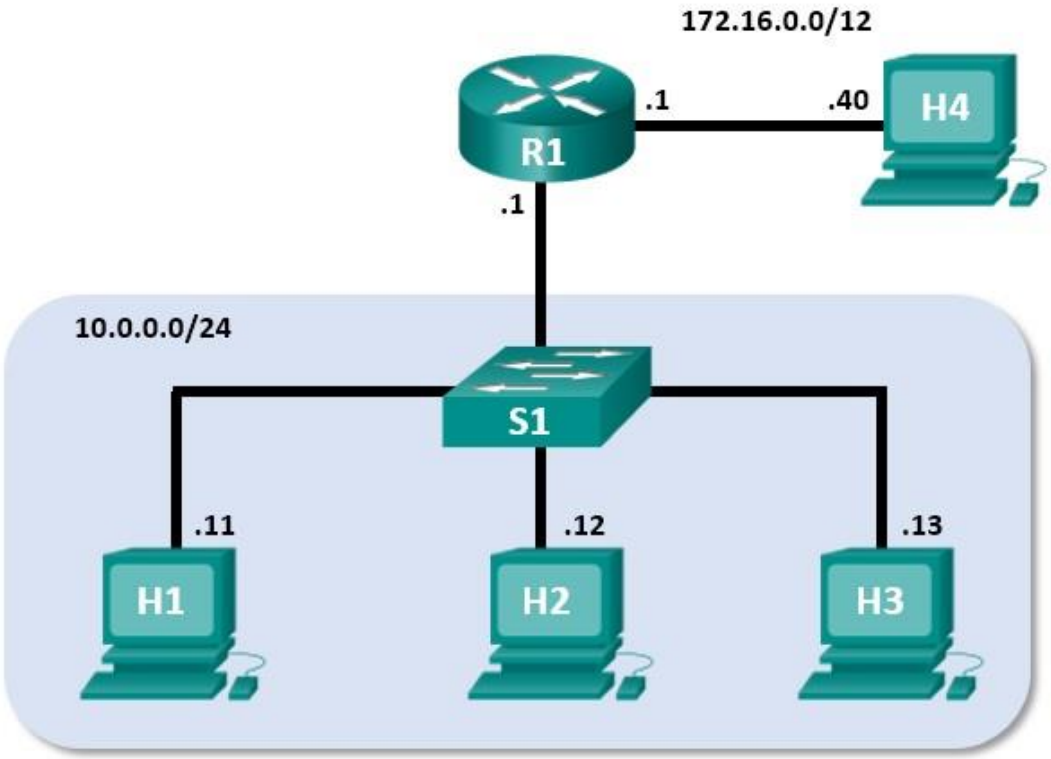
Travaux pratiques – Utiliser Wireshark pour examiner les trames Ethernet

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 virtuel CyberOps
- Accès Internet

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

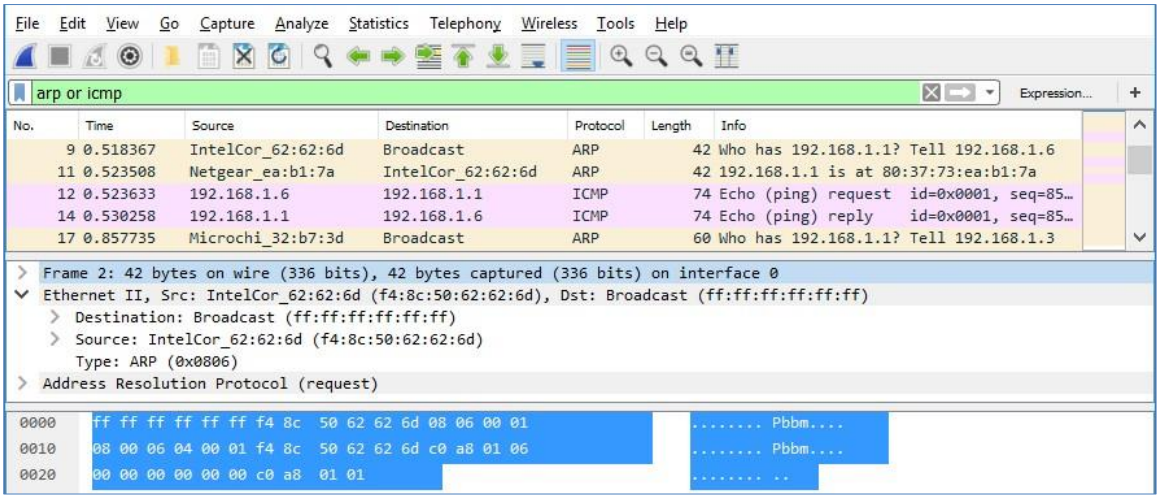
Dans la première partie, vous allez examiner les champs d'en-tête et le contenu d'une trame Ethernet II qui vous est fournie. Une capture Wireshark sera utilisée pour examiner le contenu de ces champs.

Étape 1 : 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

Étape 2 : 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.



Étape 3 : 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	Diffusion (ff:ff:ff:ff:ff:ff)	

Adresse source	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` Protocole IPv4 `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.

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

Adresse de l'Ipv6

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

Car il a besoin de savoir l'adresse MAC de l'ordinateur auquel il envoie le ping.

Quelle est l'adresse MAC de la source dans la première trame ? f4:8c:50:62:62:6d

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

À quelle partie de l'adresse MAC correspond l'identifiant OUI ? Les 4 premiers octets

Quel est le numéro de série de la carte réseau source ? 62:62:6d

Partie 2 : 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.

Étape 1 : Étudiez la configuration réseau de H3.

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

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

b. 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:
```

c. 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
```

d. À l'invite Node : h3, saisissez **ifconfig** pour vérifier l'adresse IPv4 et enregistrez l'adresse MAC.

Host-interface	Adresse IP	Adresse MAC
H3-eth0	10.0.0.13	8e:cf:fd:c0:52:76

e. 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
```

f. Quelle est l'adresse IP de la passerelle par défaut pour l'hôte H3 ? 10.0.0.1

Étape 2 : Videz le cache ARP cache sur H3 et commencez à capturer le trafic sur H3-eth0.

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

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

b. 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
```

c. 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 &
```

Étape 3 : Envoyez une requête ping H1 depuis H3.

a. 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
```

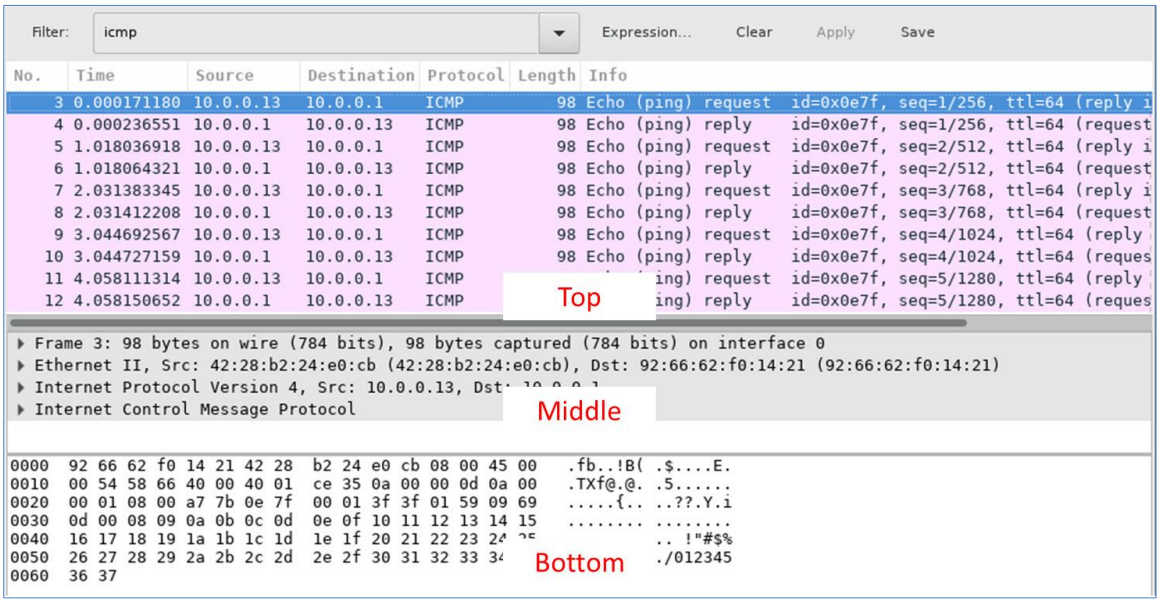
b. Une fois la requête ping terminée, arrêtez la capture Wireshark.

Étape 4 : Filtrez Wireshark pour afficher uniquement le trafic ICMP.

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

Étape 5 : 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.



a. Dans le volet Packet List (section supérieure), cliquez sur la première trame répertoriée. **Echo (ping) request** devrait s'afficher en dessous de l'en-tête **Info**. La ligne devrait également être surlignée en bleu.

b. Examinez la première ligne du volet Packet Details (section centrale). Cette ligne indique la longueur de la trame : 98 octets dans cet exemple.

c. 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.

Quelle est l'adresse MAC de la carte réseau de l'ordinateur ? de:77:b3:29:74:e6

Quelle est l'adresse MAC de la passerelle par défaut ? 8e:cd:fd:c0:52:76

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

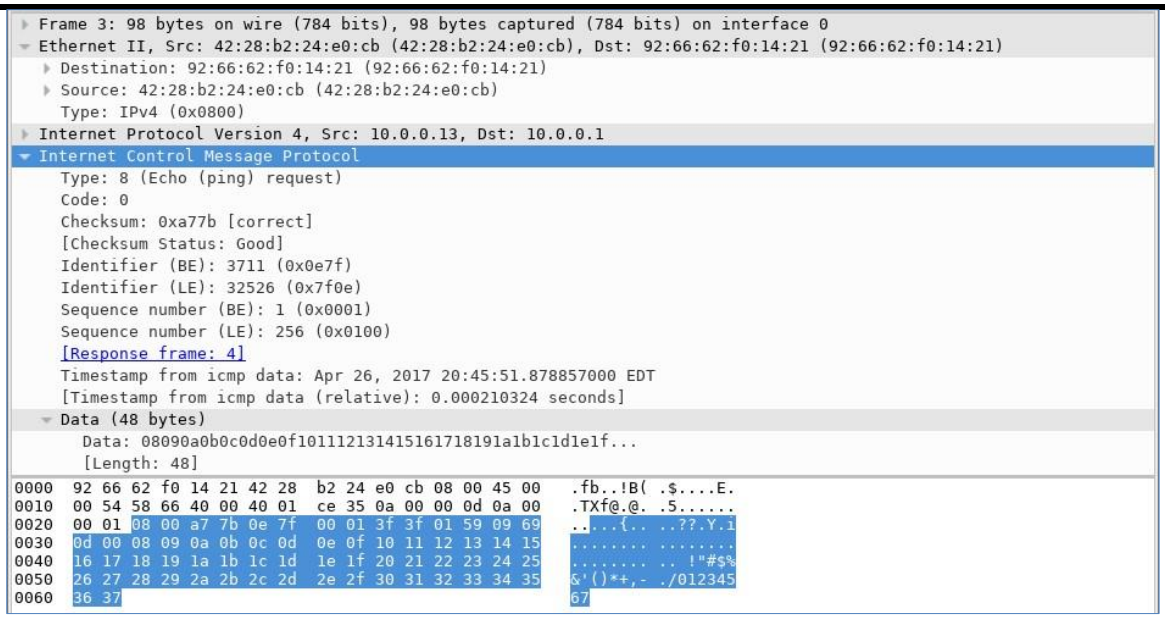
Quel type de trame est affiché ? Type IPv4

e. 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.

Quelle est l'adresse IP source ? 10.0.0.13

Quelle est l'adresse IP de destination ? 10.0.0.1

f. 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.



g. 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.

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

Le périphérique est un ordinateur avec une carte réseau Intel et une adresse MAC 8e:cd:fd:c0:52:76

Étape 6 : Lancez une nouvelle capture dans Wireshark.

a. 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).

b. Dans la fenêtre du terminal de Node : H3, envoyez 5 paquets de requêtes d'écho à 172.16.0.40.

c. Arrêtez la capture des paquets une fois les requêtes ping terminées.

Étape 7 : Examinez les nouvelles données dans le volet de la liste des paquets de Wireshark.

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

Source :

8e:cd:fd:c0:52:76

Destination :

de:77:b3:29:74:e6

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

Source :

10.0.0.13

Destination :

172.16.0.40

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

L'adresse IP de destination a changé car on questionne le router depuis le réseau interne à l'étape 5 alors que maintenant nous le questionnons depuis le réseau externe mais c'est le même appareil.

Remarques générales

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

Le champ de préambule indique que la trame arrive et permet à l'expéditeur et au récepteur d'établir une connexion.