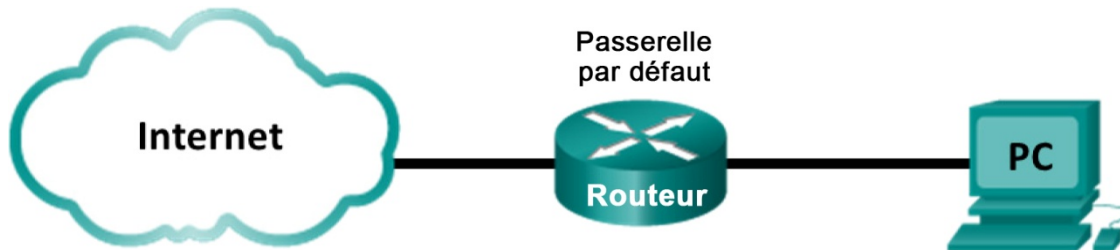


Travaux pratiques - Utilisation de Wireshark pour examiner les trames Ethernet

Topologie



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

- 1 ordinateur (Windows 7 ou 8, doté d'un accès à Internet et sur lequel Wireshark est installé)

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. 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 la configuration réseau de l'ordinateur.

L'adresse IP de cet ordinateur hôte est 192.168.1.17 et celle de la passerelle par défaut est 192.168.1.1.

```
Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Broadcom 802.11a/b/g WLAN
Physical Address. . . . . : 00-1A-73-EA-63-8C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%13(Preferred)
IPv4 Address. . . . . : 192.168.1.17(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, June 16, 2015 6:59:54 AM
Lease Expires . . . . . : Wednesday, June 17, 2015 6:59:54 AM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 234887795
DHCPv6 Client DUID. . . . . : 00-01-00-01-1B-07-0A-E1-00-1E-EC-15-74-C2

DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

Étape 3: 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.

No.	Time	Source	Destination	Protocol	Length	Info
9	2.497611000	GemtekTe_ea:63:8c	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.17
10	2.502719000	Netgear_ea:b1:7a	GemtekTe_ea:63:8c	ARP	42	192.168.1.1 is at 80:37:73:ea:b1:7a
11	2.502767000	192.168.1.17	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864,
12	2.503610000	192.168.1.1	192.168.1.17	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864,
14	3.499098000	192.168.1.17	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120,
15	3.501917000	192.168.1.1	192.168.1.17	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120,

Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)

Type: ARP (0x0806)

Address Resolution Protocol (request)

0000	ff ff ff ff ff ff 00 1a 73 ea 63 8c 08 06 00 01 S.C.....
0010	08 00 06 04 00 01 00 1a 73 ea 63 8c c0 a8 01 11 S.C.....
0020	00 00 00 00 00 00 c0 a8 01 01

Étape 4: 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)	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.						
Adresse source	GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)							
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 : <table><tr><th>Valeur</th><th>Description</th></tr><tr><td>0x0800</td><td>Protocole IPv4</td></tr><tr><td>0x0806</td><td>Protocole ARP (Address Resolution Protocol)</td></tr></table>	Valeur	Description	0x0800	Protocole IPv4	0x0806	Protocole ARP (Address Resolution Protocol)
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 ?

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

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

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

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

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

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.

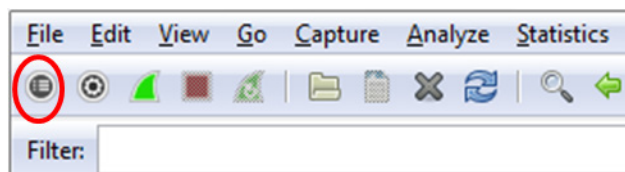
Étape 1: Déterminez l'adresse IP de la passerelle par défaut sur votre ordinateur.

Ouvrez une fenêtre d'invite de commandes et entrez la commande **ipconfig**.

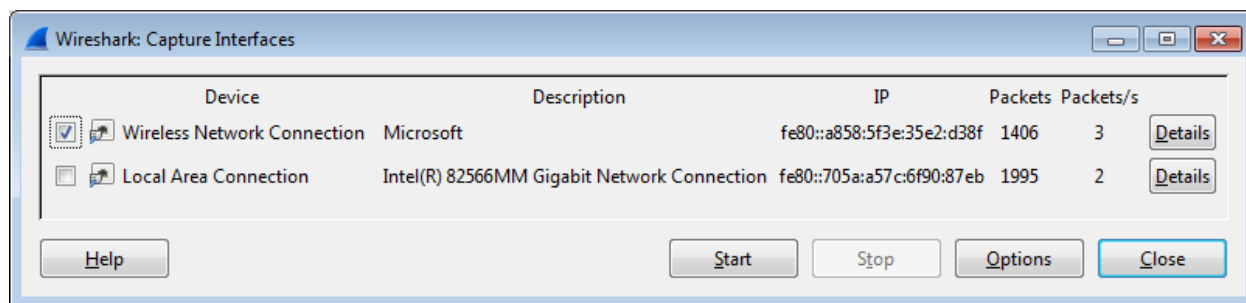
Quelle est l'adresse IP de la passerelle par défaut de l'ordinateur ? _____

Étape 2: Commencez par capturer le trafic sur la carte réseau de votre ordinateur.

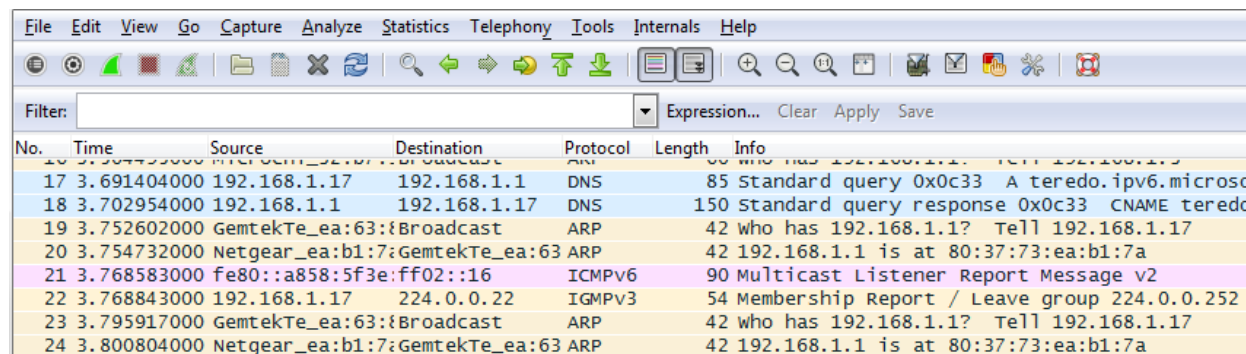
- Ouvrez Wireshark.
- Dans la barre d'outils de Wireshark Network Analyzer (outil d'analyse de réseaux Wireshark), cliquez sur l'icône **Interface List** (liste des interfaces).



- Dans la fenêtre Wireshark: Capture Interfaces (capturer des interfaces), sélectionnez l'interface pour commencer la capture du trafic en cochant la case appropriée, puis cliquez sur **Start** (démarrer). Si vous n'êtes pas sûr de l'interface à vérifier, cliquez sur **Details** (détails) pour obtenir plus d'informations sur chaque interface répertoriée.



- Observez le trafic qui apparaît dans la fenêtre Packet List (liste des paquets).

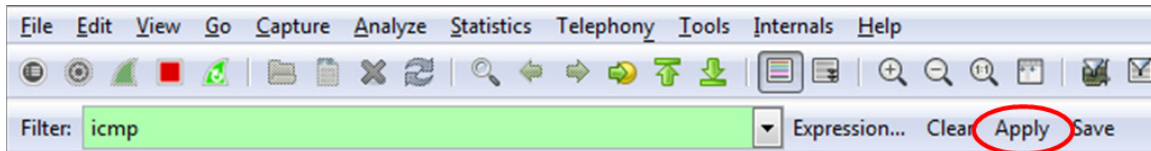


No.	Time	Source	Destination	Protocol	Length	Info
17	3.691404000	192.168.1.17	192.168.1.1	DNS	85	Standard query 0x0c33 A teredo.ipv6.microso
18	3.702954000	192.168.1.1	192.168.1.17	DNS	150	Standard query response 0x0c33 CNAME teredo
19	3.752602000	GemtekTe_ea:63::ff02::16	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.17
20	3.754732000	Netgear_ea:b1:7:GemtekTe_ea:63	ARP	ARP	42	192.168.1.1 is at 80:37:73:ea:b1:7a
21	3.768583000	fe80::a858:5f3e:ff02::16	ICMPv6	ICMPv6	90	Multicast Listener Report Message v2
22	3.768843000	192.168.1.17	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
23	3.795917000	GemtekTe_ea:63::ff02::16	ARP	ARP	42	who has 192.168.1.1? Tell 192.168.1.17
24	3.800804000	Netgear_ea:b1:7:GemtekTe_ea:63	ARP	ARP	42	192.168.1.1 is at 80:37:73:ea:b1:7a

Étape 3: Filtrez Wireshark pour afficher uniquement le trafic ICMP.

Vous pouvez utiliser le filtre dans Wireshark pour bloquer la visibilité du trafic indésirable. Le filtre ne bloque pas la capture des données indésirables ; il filtre uniquement ce qui doit s'afficher à l'écran. Pour le moment, seul le trafic ICMP doit être affiché.

Dans la zone **Filter** (filtre) de Wireshark, saisissez **icmp**. La case devient verte si vous avez correctement tapé le filtre. Si la case est verte, cliquez sur **Apply** (appliquer) pour appliquer le filtre.

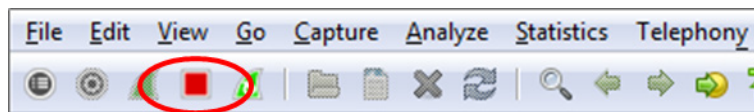


Étape 4: À partir de la fenêtre d'invite de commandes, envoyez une requête ping à la passerelle par défaut de votre ordinateur.

À partir de la fenêtre de commandes, envoyez une requête ping à la passerelle par défaut avec l'adresse IP que vous avez notée à l'étape 1.

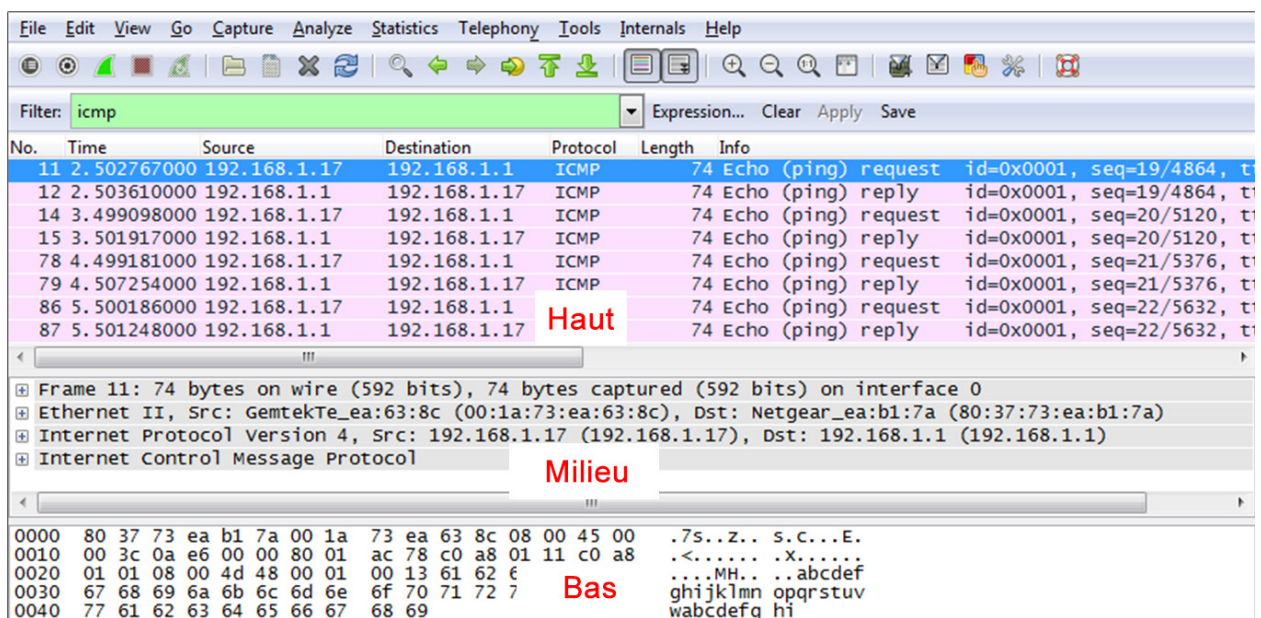
Étape 5: Arrêtez la capture du trafic sur la carte réseau.

Cliquez sur l'icône **Stop Capture** (arrêter la capture) pour arrêter la capture du trafic.



Étape 6: 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.



- 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.
- Examinez la première ligne du volet Packet Details (section centrale). Cette ligne indique la longueur de la trame : 74 octets dans cet exemple.
- 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 ? _____
Quelle est l'adresse MAC de la passerelle par défaut ? _____
- Vous pouvez cliquer sur le signe plus (+) au début de la deuxième ligne afin d'obtenir des informations supplémentaires sur la trame Ethernet II. Notez que le signe plus devient un signe moins (-).
Quel type de trame est affiché ? _____
- 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 ? _____
Quelle est l'adresse IP de destination ? _____
- 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.

The screenshot shows the Wireshark interface with the following details:

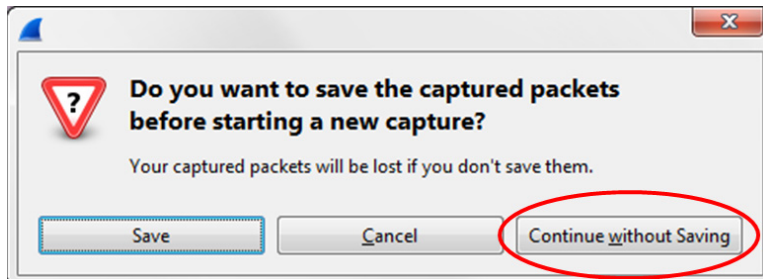
- Packet List:** Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Packet Details:**
 - Ethernet II, Src: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)
 - Source: GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)
 - Type: IP (0x0800)
 - Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 192.168.1.1 (192.168.1.1)
 - Internet Control Message Protocol**
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0x4d48 [correct]
- Packet Bytes:**

0000	80 37 73 ea b1 7a 00 1a 73 ea 63 8c 08 00 45 00	.7s..Z..S.C...E.
0010	00 3c 0a e6 00 00 80 01 ac 78 c0 a8 01 11 c0 a8	.<.....X.....
0020	01 01 08 00 4d 48 00 01 00 13 61 62 63 64 65 66	..MH.. ..abcder
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcdefg hi

- Quelles sont les deux dernières lettres des octets mis en surbrillance ? _____
- 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 ? _____

Étape 7: Redémarrez la capture de paquets dans Wireshark.

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).



Étape 8: Dans la fenêtre d'invite de commandes, envoyez une requête ping à www.cisco.com.

Étape 9: Arrêtez la capture des paquets.

Étape 10: 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 : _____

Destination : _____

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 6. 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 ?

Remarques générales

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