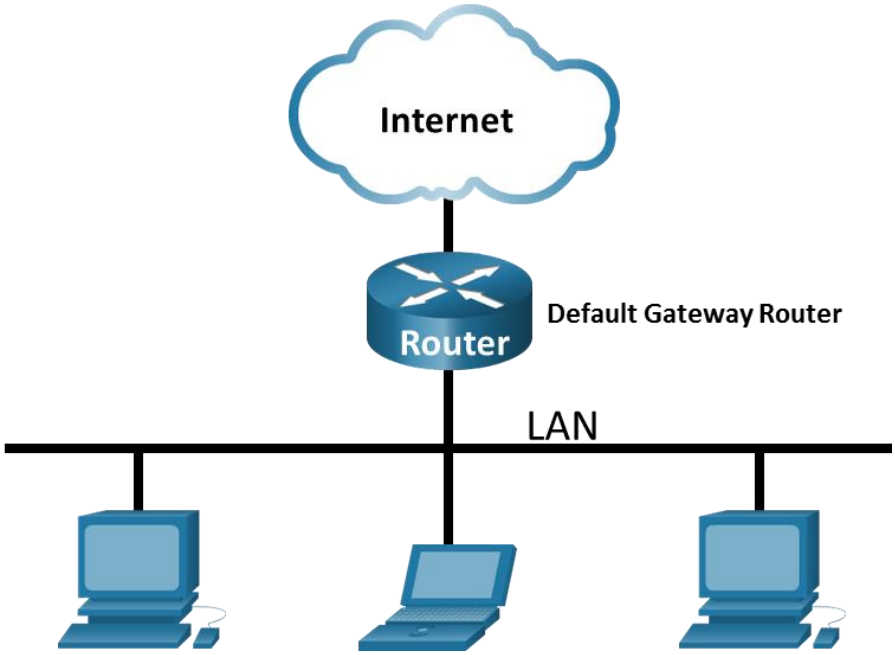
Travaux pratiques - Utilisation de Wireshark pour voir le trafic réseau

(Version de l'instructeur)

Remarque du formateur : le texte en rouge ou surligné en gris apparaît uniquement dans la version du formateur.

Topologie



Objectifs

Partie 1: Capturer et analyser les données ICMP locales avec Wireshark

Partie 2: Capturer et analyser les données ICMP distantes avec Wireshark

Contexte/Scénario

Wireshark est un analyseur de protocoles (analyseur de paquets) utilisé pour dépanner les réseaux, effectuer des analyses, développer des logiciels et des protocoles et s'informer. L'analyseur «capture» chaque unité de données de protocole (PDU) des flux de données circulant sur le réseau. Il permet de décoder et d'analyser leur contenu conformément aux spécifications RFC ou autres appropriées.

Wireshark est un outil qui est utile pour toutes les personnes intervenant au niveau des réseaux. Vous pouvez vous en servir dans le cadre de la plupart des travaux pratiques des cours CCNA, à fins d'analyse de données et de dépannage. Au cours de ces travaux pratiques, vous utiliserez Wireshark pour capturer les adresses IP des paquets de données ICMP et les adresses MAC de trames Ethernet.

Ressources requises

- 1 ordinateur (Windows avec accès Internet)
- Des ordinateurs supplémentaires sur un réseau local (LAN) seront utilisés pour répondre aux requêtes ping.

Remarque du formateur:ces travaux pratiques supposent que l'étudiant utilise un PC disposant d'un accès à Internet et qu'il est capable d'envoyer des requêtes ping aux autres PC du réseau local.

L'utilisation d'un analyseur de paquets tel que Wireshark peut constituer une infraction à la stratégie de sécurité de l'établissement de formation. Nous vous recommandons d'obtenir une autorisation avant d'exécuter Wireshark dans le cadre de ces travaux pratiques. Si l'utilisation d'un analyseur de paquets tel que Wireshark pose problème, le formateur peut proposer aux étudiants d'effectuer les travaux pratiques chez eux ou de réaliser une démonstration virtuelle.

Instructions

Partie 1: Capturer et analyser les données ICMP locales avec Wireshark

Dans la partie 1 de ces travaux pratiques, vous exécuterez une commande ping sur un autre ordinateur du réseau local (LAN) et capturerez des requêtes et des réponses ICMP dans Wireshark. Vous examinerez également les trames capturées pour obtenir des informations spécifiques. Cette analyse devrait vous aider à mieux comprendre la façon dont les en-têtes de paquet sont utilisés pour transporter les données vers leur destination.

Étape 1: Récupérez les adresses d'interface de votre ordinateur.

Dans le cadre de ces travaux pratiques, il vous faudra récupérer l'adresse IP de votre ordinateur et l'adresse physique de sa carte réseau, également appelée adresse MAC.

a. Ouvrez une fenêtre de commandes, tapez **ipconfig /all**, puis appuyez sur Entrée, Notez l'adresse IP de l'interface de votre ordinateur, sa description et son adresse MAC (physique).

```
C:\Users\Student> ipconfig /renew

Configuration IP Windows

   Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC
   Primary Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : Non
   IP Routing Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
```

```
   Description . . . . . . . . . . . : Intel(R) 82577LC Gigabit Network Connection
   Physical Address. . . . . . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : Non
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80 : :d809:d 939:110 f:1b7f%20 (Préféré)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
<output omitted>
```

b. Demandez à un ou plusieurs membres de l'équipe de fournir l'adresse IP de leur ordinateur et leur donnez l'adresse IP de votre ordinateur. Ne lui fournissez pas votre adresse MAC pour le moment.

Étape 2: Démarrez Wireshark et commencez à capturer des données.

a. Accédez à Wireshark. Double-cliquez sur l'interface souhaitée pour démarrer la capture de paquets. Assurez-vous que l'interface souhaitée a du trafic.

b. Les informations commencent à défiler vers le bas à partir de la section supérieure dans Wireshark. Les lignes de données s'affichent en différentes couleurs selon le protocole.

   Ces informations peuvent défiler très rapidement selon la nature des communications survenant entre votre ordinateur et le réseau local (LAN). Nous pouvons appliquer un filtre pour faciliter l'affichage et la manipulation des données capturées par Wireshark.

   Dans le cadre de ces travaux pratiques, nous nous concentrerons uniquement sur l'affichage des unités de données de protocole (PDU) (ping) ICMP. Tapez **icmp** dans la zone **Filter** en haut de Wireshark et appuyez sur **Entrée** ou cliquez sur le bouton **Apply** (flèche) pour afficher uniquement les unités de données de protocole (PDU) (ping) ICMP.

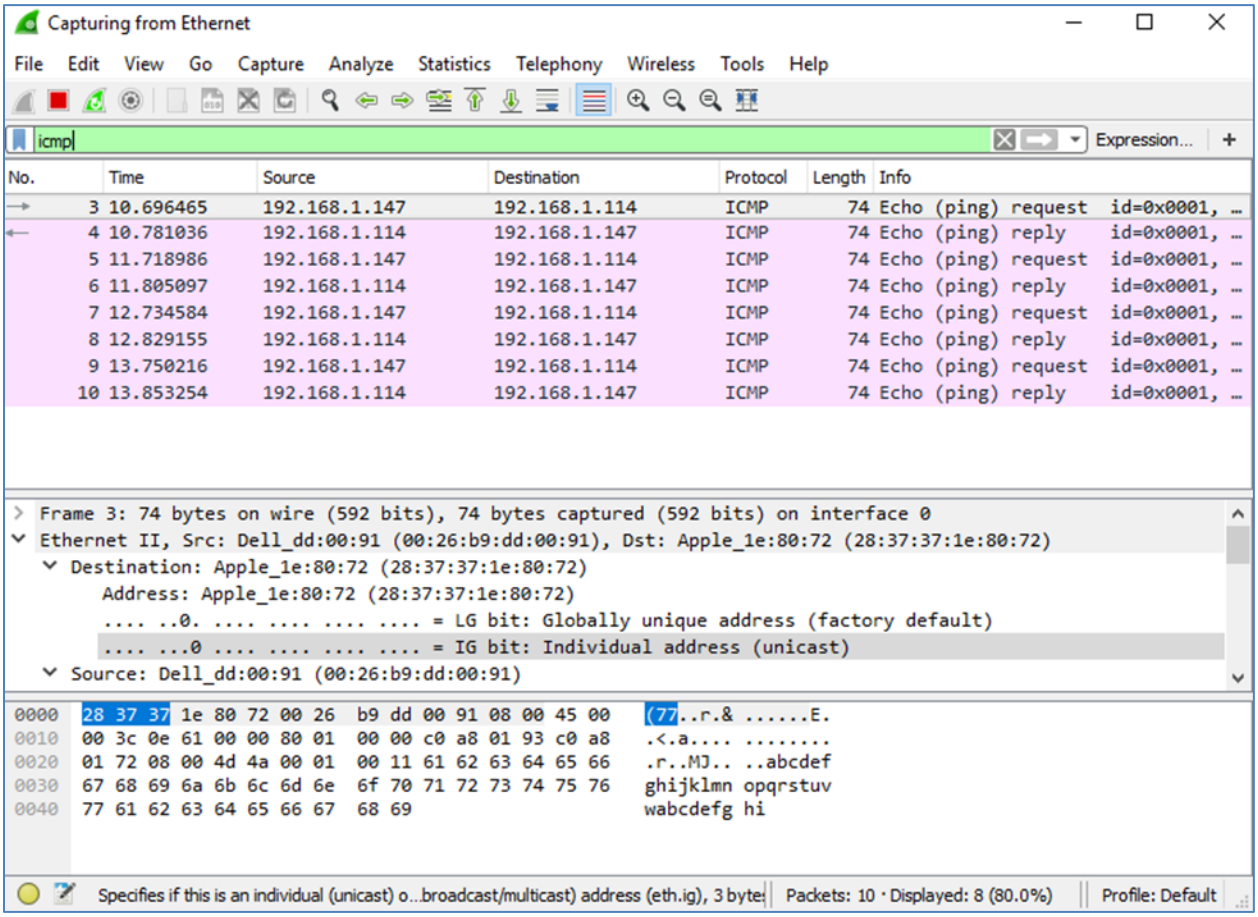
c. Ce filtre fait disparaître toutes les données de la fenêtre supérieure, mais la capture du trafic dans l'interface se poursuit. Accédez à la fenêtre d'invite de commandes et envoyez une requête ping à l'adresse IP que vous avez reçue du membre de votre équipe.

```
C:\ > ping 192.168.1.114

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum=0ms, Maximum=0ms, Moyenne=0ms
```

Notez que les données commencent à apparaître à nouveau dans la fenêtre supérieure de Wireshark.



Remarque: Si l'ordinateur du membre de votre équipe ne répond pas aux requêtes ping, c'est qu'elles sont peut-être bloquées par le par-feu de son ordinateur. Consultez l'Annexe A: Autoriser le trafic ICMP via un pare-feu information pour savoir comment autoriser le trafic ICMP via le pare-feu en utilisant Windows.

d. Arrêtez la capture des données en cliquant sur l'icône **Stop Capture** (Arrêter la capture).

Étape 3: Examinez les données capturées.

À l'étape 3, examinez les données qui ont été générées par les requêtes ping de l'ordinateur du membre de votre équipe. Les données Wireshark s'affichent dans trois sections : 1) la section supérieure affiche la liste des trames PDU capturées avec un résumé des informations de paquet IP, 2) la section centrale liste les informations PDU correspondant à la trame sélectionnée dans la partie supérieure de l'écran et fractionne une trame PDU capturée en fonction de ses couches de protocole, et 3) la section du bas affiche les données brutes de chaque couche. Les données brutes sont affichées sous forme hexadécimale et décimale.

a. Cliquez sur les premières trames PDU de requête ICMP dans la partie supérieure de Wireshark. Notez que la colonne **Source** contient l'adresse IP de votre ordinateur, tandis que la colonne **Destination** contient l'adresse IP de l'ordinateur de votre équipier auquel vous avez envoyé des requêtes ping.

b. Tandis que cette trame PDU est toujours sélectionnée dans la partie supérieure, accédez à la partie centrale. Cliquez sur le signe plus à gauche de la ligne Ethernet II pour afficher les adresses MAC de destination et source.

L'adresse MAC source correspond-elle à l'interface de votre ordinateur?

Oui

L'adresse MAC de destination dans Wireshark correspond-elle à celle de l'ordinateur du membre de votre équipe ?

Oui

Comment votre ordinateur obtient-il l'adresse MAC de l'ordinateur destinataire des requêtes ping ?

L'adresse MAC est obtenue par le biais d'une requête ARP.

Remarque: dans l'exemple précédent d'une requête ICMP capturée, les données ICMP sont encapsulées dans une unité de données de protocole (PDU) de paquet IPv4 (en-tête IPv4) qui est ensuite encapsulée dans une PDU de trame Ethernet II (en-tête Ethernet II) en vue de sa transmission sur le réseau local (LAN).

Partie 2: Capturer et analyser les données ICMP distantes avec Wireshark

Dans la partie 2, vous enverrez des requêtes ping aux hôtes distants (les hôtes ne figurant pas sur le réseau local (LAN)) et vous examinerez les données générées à partir de ces requêtes ping. Ensuite, vous déterminerez en quoi ces données diffèrent des données examinées dans la partie 1.

Étape 1: Commencez par capturer les données sur l'interface.

a. Lancez à nouveau la capture des données.

b. Une fenêtre vous invite à enregistrer les données capturées précédemment avant de commencer une autre capture. Il n'est pas nécessaire d'enregistrer ces données. Cliquez sur **Continue without Saving** (Continuer sans enregistrer).

c. Le processus de capture étant actif, envoyez une requête ping aux trois URL de sites web suivantes :

1) www.yahoo.com

2) www.cisco.com

3) www.google.com

Remarque: lorsque vous envoyez une requête ping aux URL indiquées, notez que le serveur de noms de domaine (DNS) traduit l'URL en adresse IP. Notez l'adresse IP reçue pour chaque URL.

d. Vous pouvez arrêter la capture des données en cliquant sur l'icône **Stop Capture** (Arrêter la capture).

Étape 2: Examen et analyse des données provenant des hôtes distants.

Examinez les données capturées dans Wireshark, examinez les adresses IP et MAC des trois emplacements auxquels vous avez envoyé des requêtes ping. Indiquez les adresses IP et MAC de destination pour les trois emplacements dans l'espace prévu à cet effet.

Adresse IP de **www.yahoo.com**:

Adresse MAC pour **www.yahoo.com**:

Adresse IP de **www.yahoo.com**:

Adresse MAC pour **www.cisco.com**:

Adresse IP pour **www.google.com**:

Adresse MAC pour **www.google.com**:

Adresses IP sont : 98.137.246.7, 96.7.79.147, 172.217.14.100 (ces adresses IP peuvent varier)

Adresse MAC : identique pour les trois emplacements. Cette entrée fournit l'adresse physique de l'interface LAN de la passerelle par défaut sur le routeur.

Qu'y a-t-il d'important à retenir de ces informations ?

Les adresses MAC de ces trois emplacements sont identiques.

En quoi ces informations diffèrent-elles des informations de requêtes ping locales que vous avez reçues dans la partie 1?

Une commande ping envoyée à un hôte local renvoie l'adresse MAC de la carte réseau de l'ordinateur. Une commande ping envoyée à un hôte distant renvoie l'adresse MAC de l'interface LAN de la passerelle par défaut.

Question de réflexion

Pourquoi Wireshark affiche-t-il l'adresse MAC réelle des hôtes locaux, mais pas l'adresse MAC réelle des hôtes distants ?

Étant donné que les adresses MAC des hôtes distants ne sont pas connues sur le réseau local, c'est l'adresse MAC de la passerelle par défaut qui est utilisée. Une fois que le paquet a atteint le routeur de

la passerelle par défaut, les informations de la couche 2 sont supprimées du paquet et un nouvel en-tête de couche 2 est relié à l'adresse MAC de destination du routeur au niveau du saut suivant.

Annexe A: Autoriser le trafic ICMP via un pare-feu

Si les membres de votre équipe ne parviennent pas à envoyer de requêtes ping à votre ordinateur, il est possible que votre pare-feu les bloque. Cette annexe explique comment créer une règle sur le pare-feu afin d'autoriser les requêtes ping. Elle décrit également comment désactiver la nouvelle règle ICMP une fois que vous avez terminé les travaux pratiques.

Partie 1: Créez une règle de trafic entrant autorisant le trafic ICMP via le pare-feu.

a. À partir du **Panneau de configuration**, cliquez sur l'option **Système et sécurité** dans la categorie Afficher.

b. Dans la fenêtre **Système et sécurité**, cliquez sur **Pare-feu Windows Defender** ou **Pare-feu Windows**.

c. Dans le volet gauche de la fenêtre **Pare-feu Windows Defender**ou **Par-feu Windows** cliquez sur **Paramètres avancés**.

d. Dans la fenêtre des **fonctions de sécurité avancées**, choisissez l'option **Règles de trafic entrant** dans la barre latérale gauche, puis cliquez sur **Nouvelle règle…** dans la barre latérale droite.

e. Cette action démarre l'Assistant **Nouvelle règle de trafic entrant**. Dans l'écran **Type de règle**, cliquez sur la case d'option **Personnalisée**, puis cliquez sur **Suivant**.

f. Dans le volet gauche, cliquez sur l'option **Protocole et ports**, et au moyen du menu déroulant **Type de protocole**, sélectionnez **ICMPv4**, puis cliquez sur **Suivant**.

g. Vérifiez que **toute adresse IP** pour les adresses IP locales et distantes est sélectionnée. Cliquez sur **Suivant** pour continuer.

h. Sélectionnez **Autoriser la connexion**. Cliquez sur **Suivant** pour continuer.

i. Par défaut, cette règle s'applique à tous les profils. Cliquez sur **Suivant** pour continuer.

j. Nommez la règle avec **Autoriser les requêtes ICMP**. Cliquez sur **Finish (Terminer)** pour continuer. Cette nouvelle règle doit permettre aux membres de votre équipe de recevoir des réponses ping de votre ordinateur.

Partie 2: Désactivation ou suppression de la nouvelle règle ICMP.

Une fois que les travaux pratiques sont terminés, vous pouvez désactiver ou même supprimer la règle que vous avez créée à l'étape 1. L'option **Désactiver la règle** vous permet d'activer la règle à nouveau plus tard. La suppression de la règle l'élimine définitivement de la liste des règles de trafic entrant.

a. Dans la fenêtre des **fonctions de sécurité avancées**, dans le volet gauche, cliquez sur **Règles de trafic entrant**, puis localisez la règle que vous avez créée à l'étape1.

b. Cliquez avec le bouton droit sur la règle ICMP et sélectionnez **Désactiver la règle** si vous le souhaitez. Vous pouvez également sélectionner **Supprimer** si vous souhaitez le supprimer définitivement. Si vous choisissez cette option, vous devez recréer la règle pour autoriser les réponses ICMP.