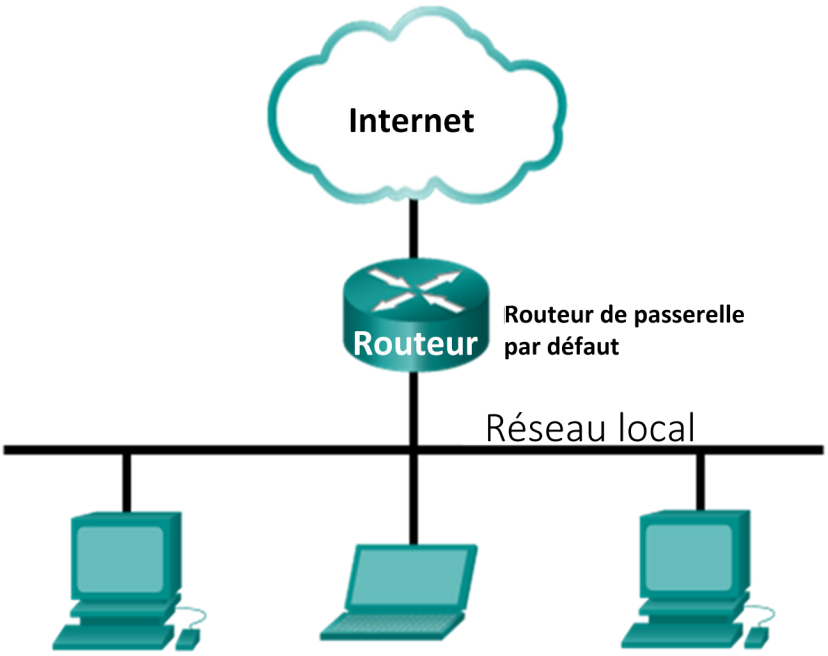
Travaux pratiques - Utilisation de Wireshark pour voir le trafic réseau

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.

Cet outil 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 des 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 7, 8 ou 10 équipé d'un accès à Internet)
- Des ordinateurs supplémentaires sur un réseau local (LAN) seront utilisés pour répondre aux requêtes ping.

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

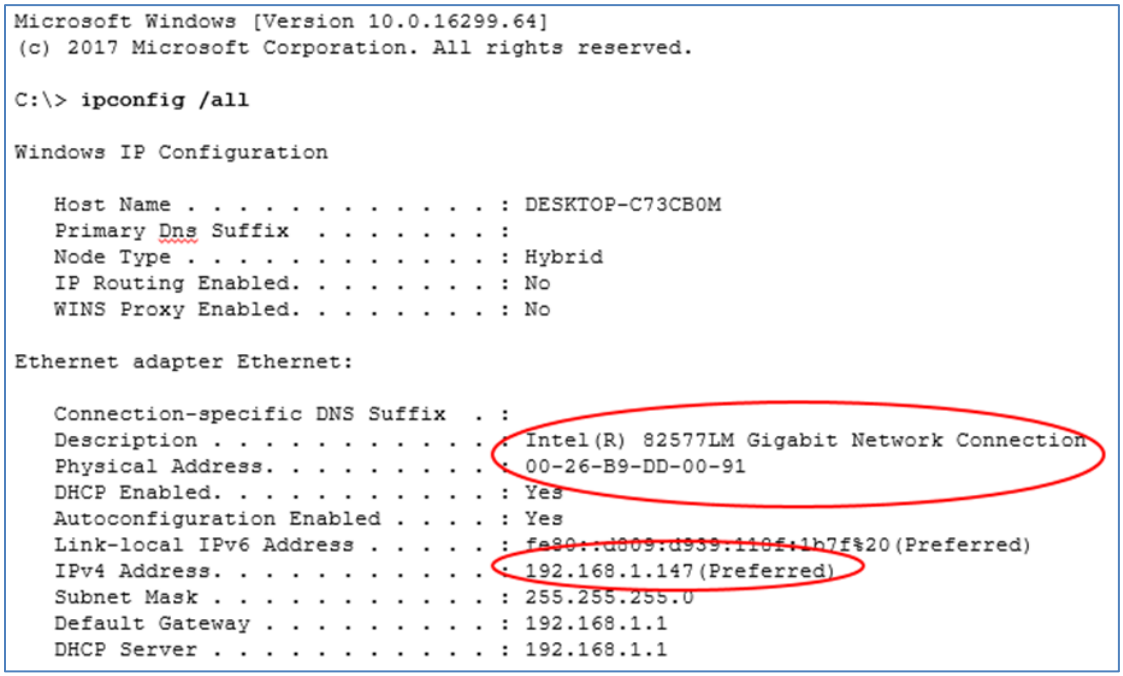
Dans la partie 1 de ces travaux pratiques, vous exécuterez une commande ping sur un autre ordinateur du réseau local (LAN) et capturerez des requêtes et des réponses ICMP dans Wireshark. Vous examinerez également les trames capturées pour obtenir des informations spécifiques. Cette analyse devrait vous 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.

b. Notez l'adresse IP de l'interface de votre ordinateur, sa description et son adresse MAC (physique).



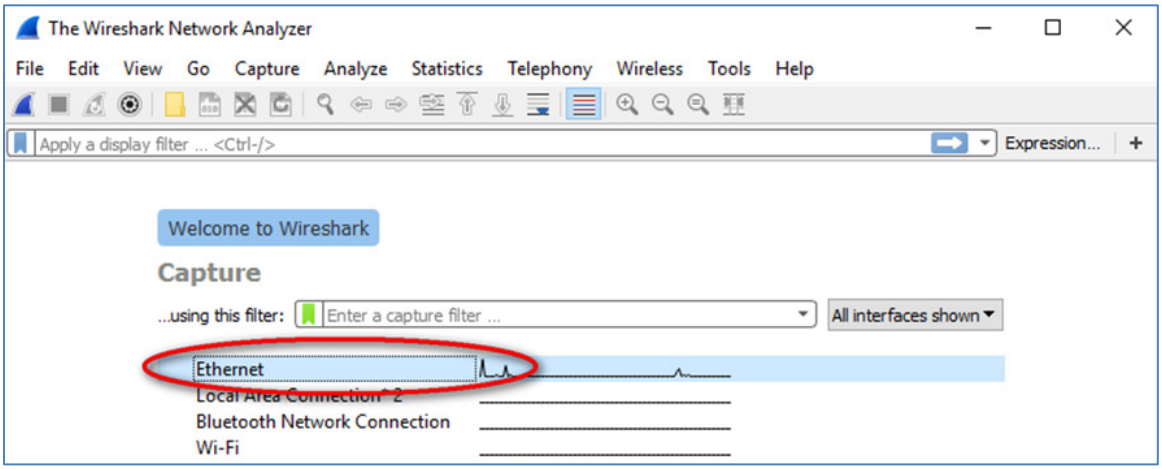
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C73CB0M
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

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

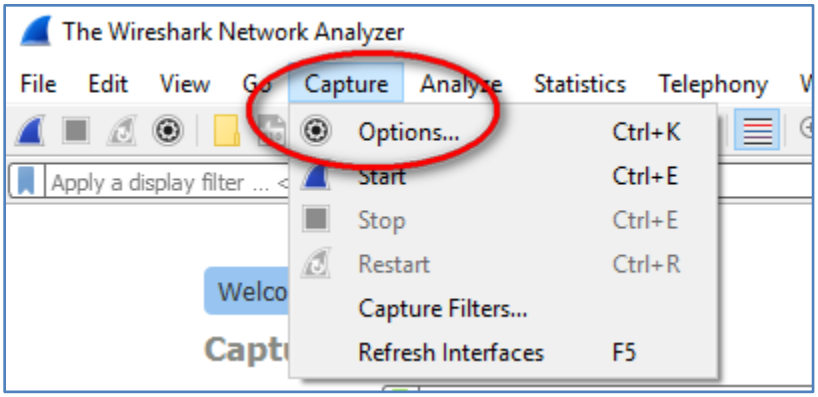
Étape 2 : Démarrez Wireshark et commencez à capturer des données.

a. Sur votre ordinateur, cliquez sur le bouton **Démarrer** de Windows pour voir s'afficher Wireshark avec les autres programmes du menu contextuel. Double-cliquez sur **Wireshark**.

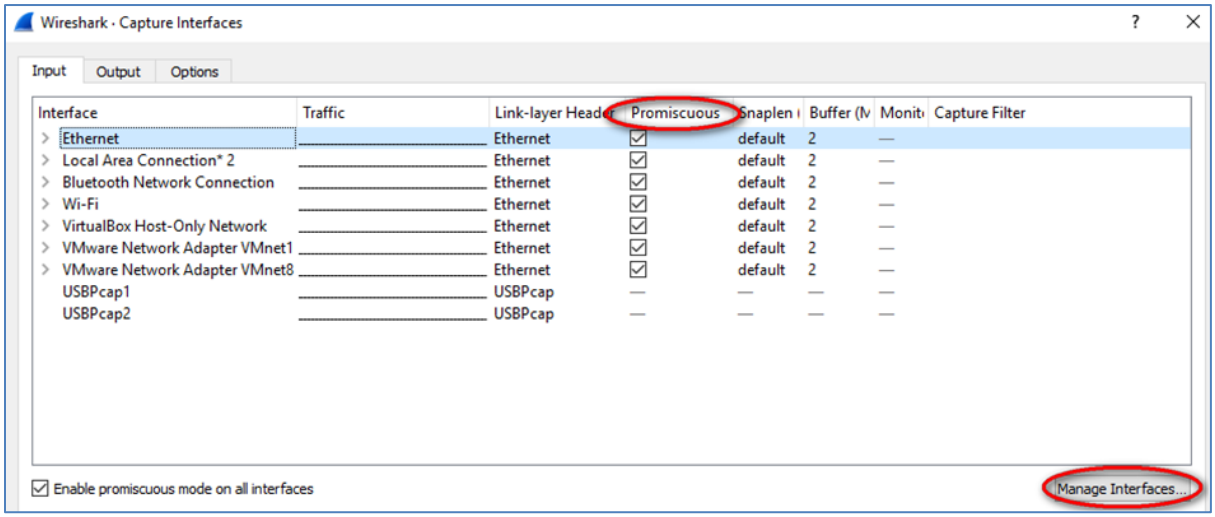
b. Une fois Wireshark démarré, cliquez sur l'interface de capture à utiliser. L'ordinateur utilisant une connexion Ethernet filaire, assurez-vous que l'option Ethernet se trouve en haut de la liste.



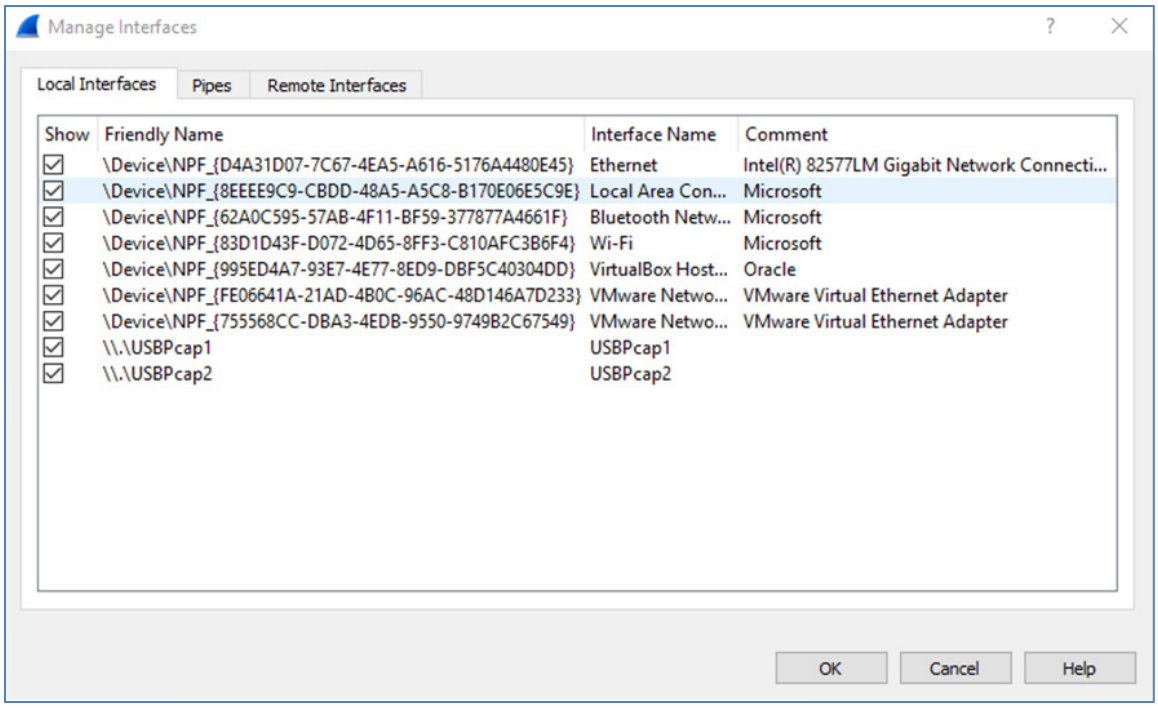
Vous pouvez gérer l'interface de capture en cliquant sur **Capture** et sur **Options** :



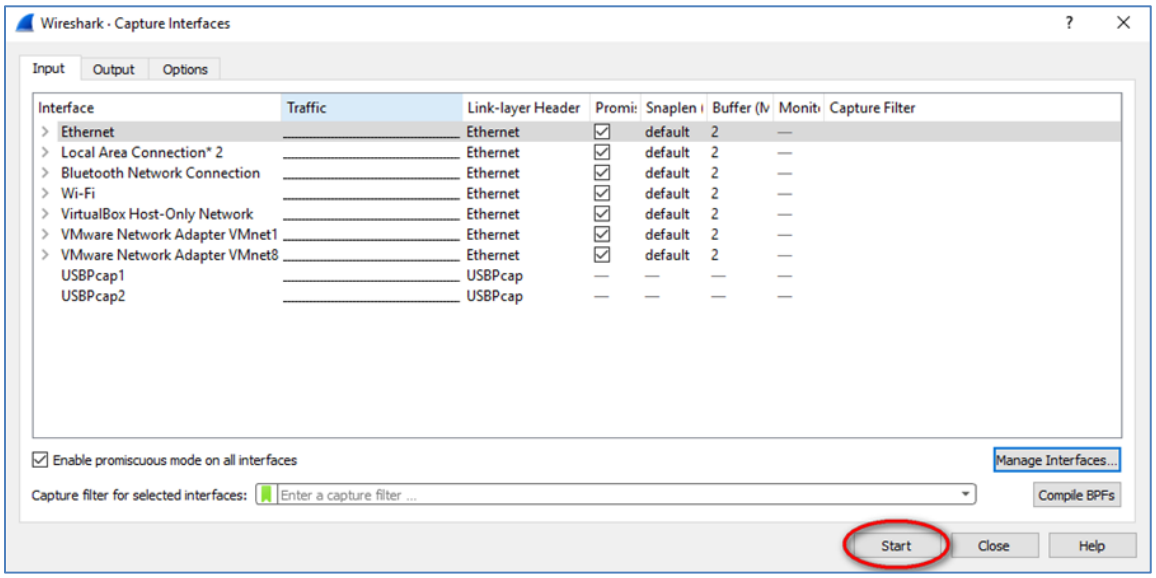
c. Une liste des interfaces s'affiche. Assurez-vous que l'interface de capture est sélectionnée sous **Promiscuous**.



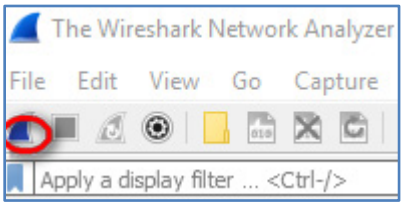
Remarque : vous pouvez contrôler davantage la gestion des interfaces sur l'ordinateur en cliquant sur **Manage Interfaces**. Vérifiez que la description correspond à ce que vous avez noté à l'étape 1b. Fermez la fenêtre **Manage Interfaces** après avoir vérifié l'interface appropriée.



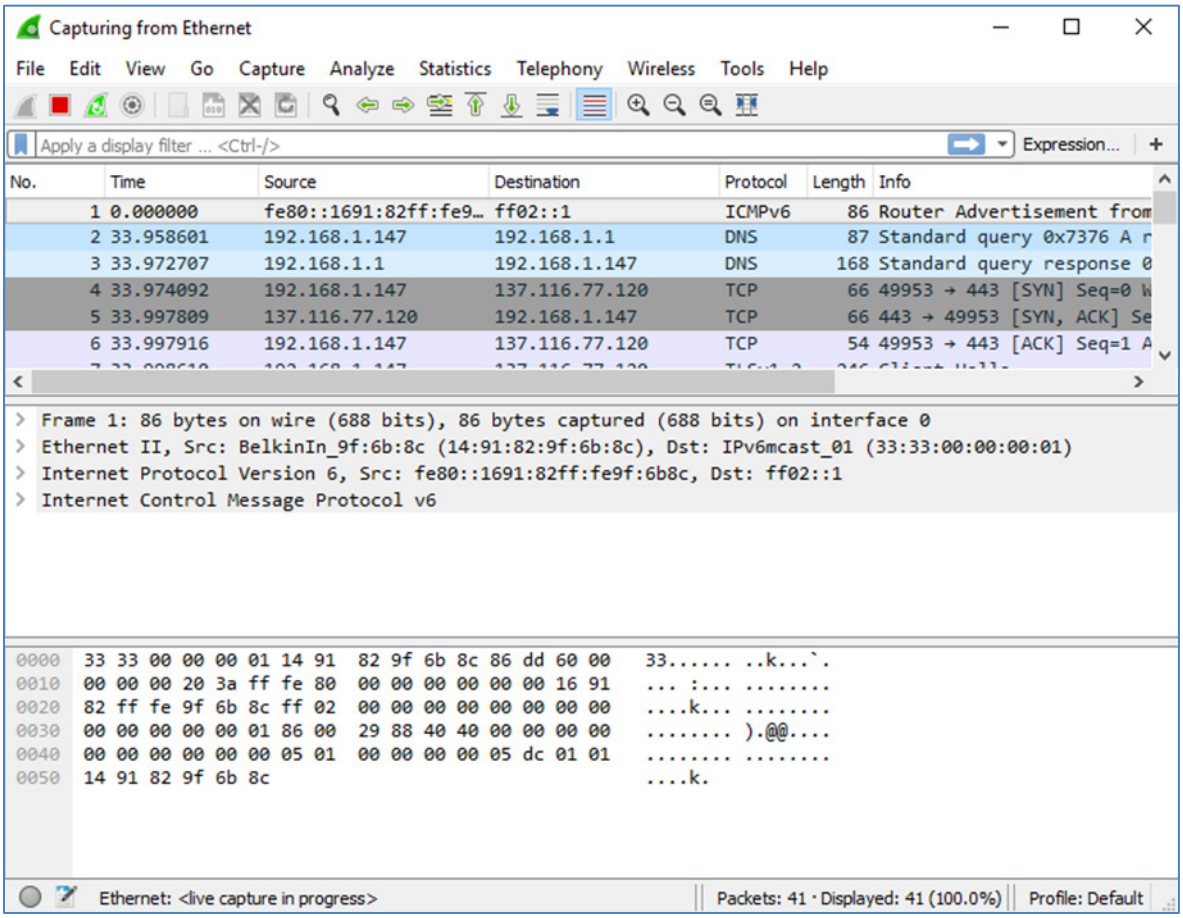
d. Après avoir sélectionné l'interface appropriée, cliquez sur **Start** (Démarrer) pour lancer la capture des données.



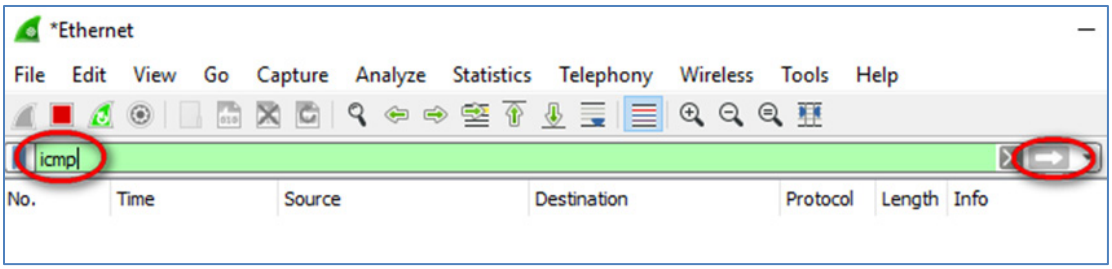
Remarque : vous pouvez également lancer la capture des données en cliquant sur l'icône **Wireshark** dans l'interface principale.



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.



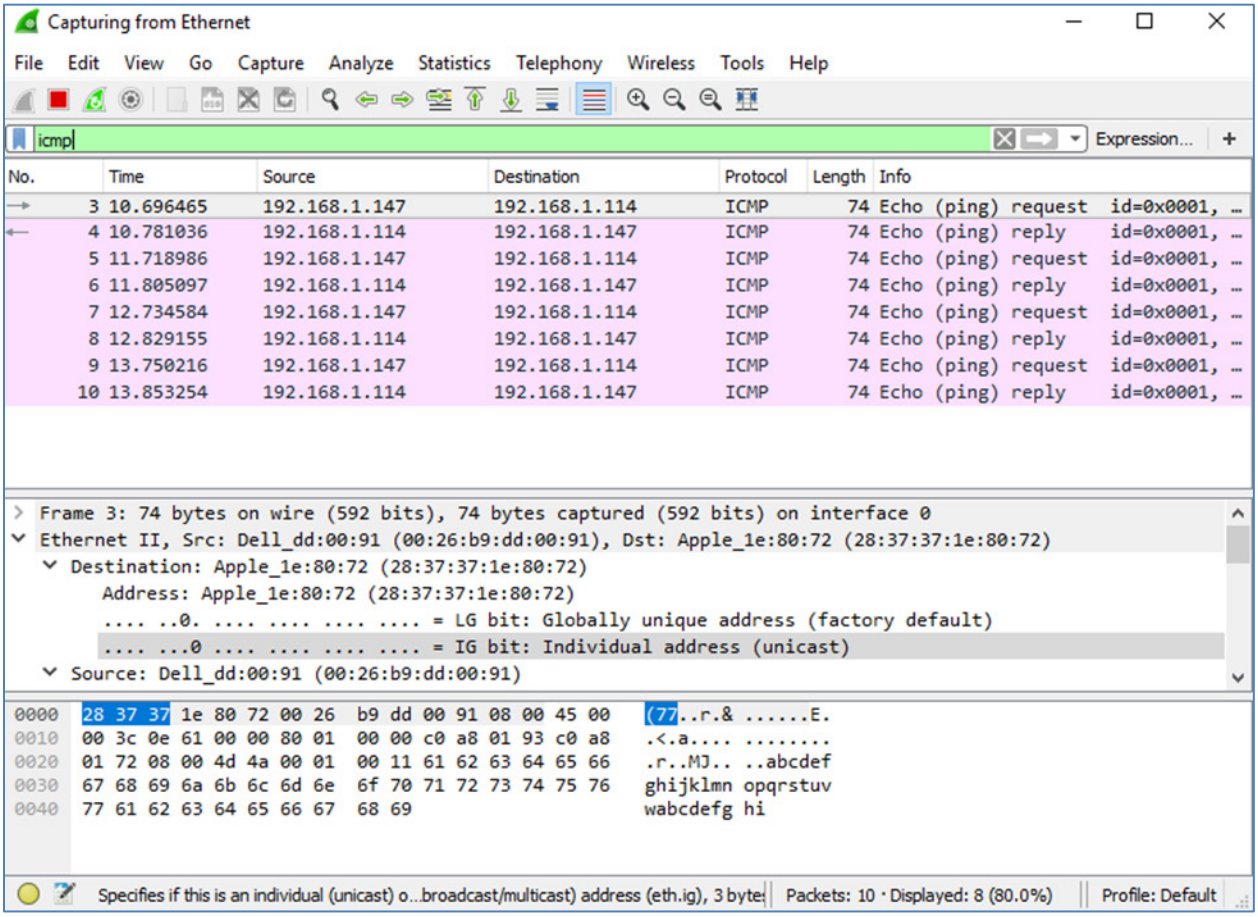
e. Ces informations peuvent défiler très rapidement selon la nature des communications survenant entre votre ordinateur et le réseau local (LAN). Nous pouvons appliquer un filtre pour faciliter l'affichage et la manipulation des données capturées par Wireshark. Dans le cadre de ces travaux pratiques,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



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

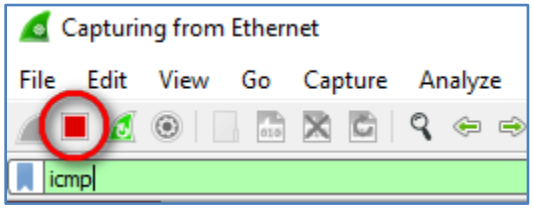
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64

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, Average = 0ms
```

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



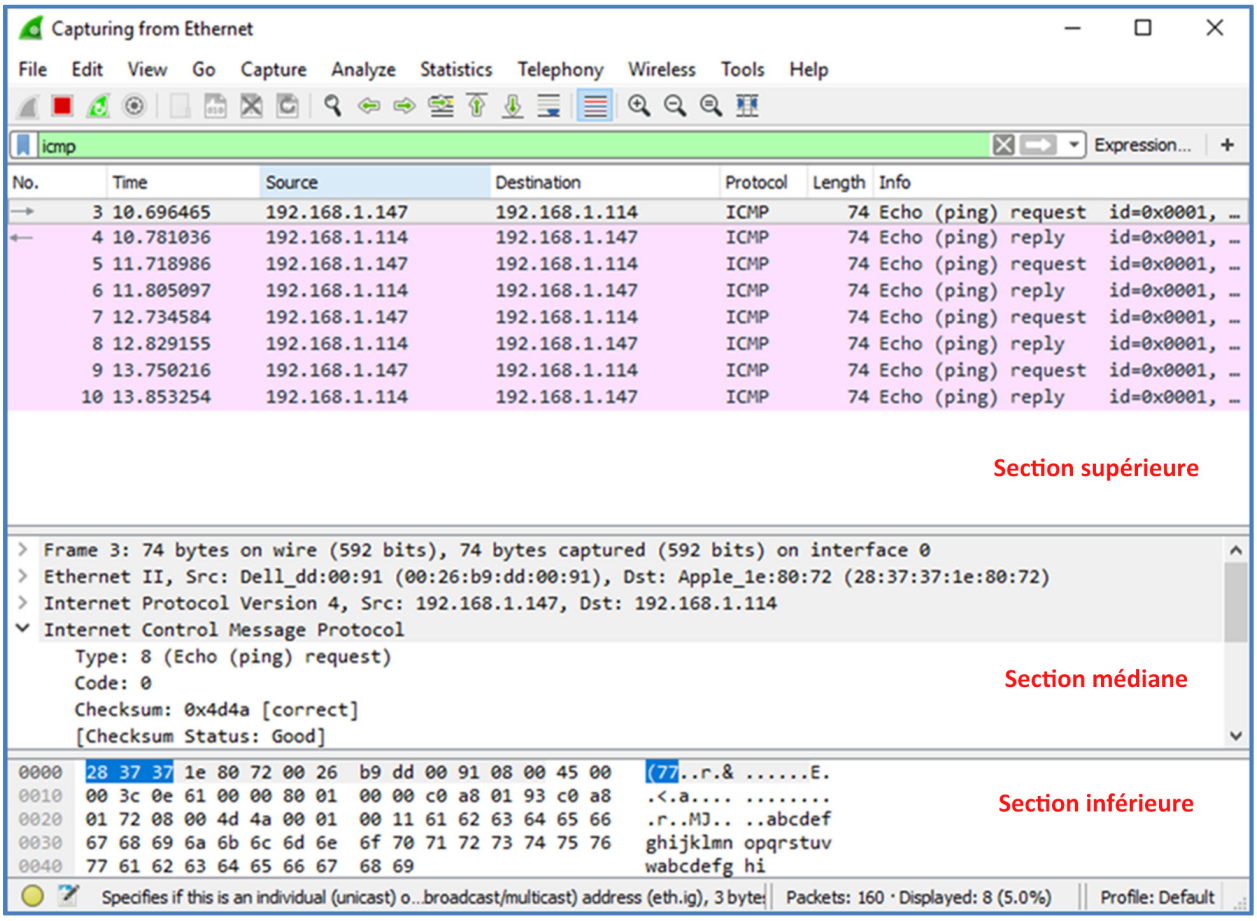
Remarque : si l'ordinateur du membre de votre équipe ne répond pas aux requêtes ping, c'est qu'elles sont peut-être bloquées par le pare-feu de son ordinateur. Consultez l'Annexe A : Autoriser le trafic ICMP via un pare-feu pour savoir comment autoriser le trafic ICMP via le pare-feu sous Windows 7.

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

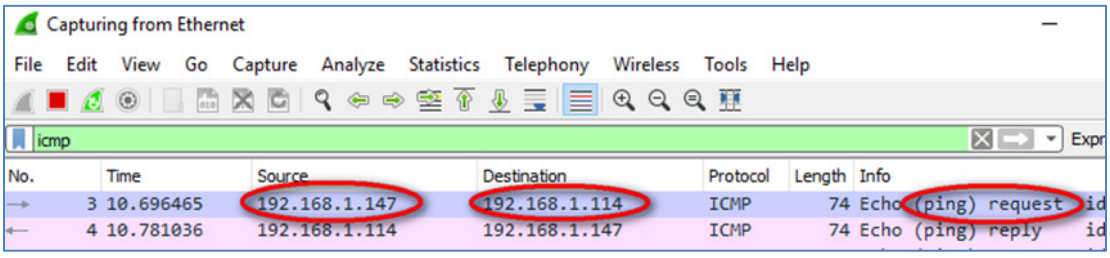


Étape 3 : Examinez les données capturées.

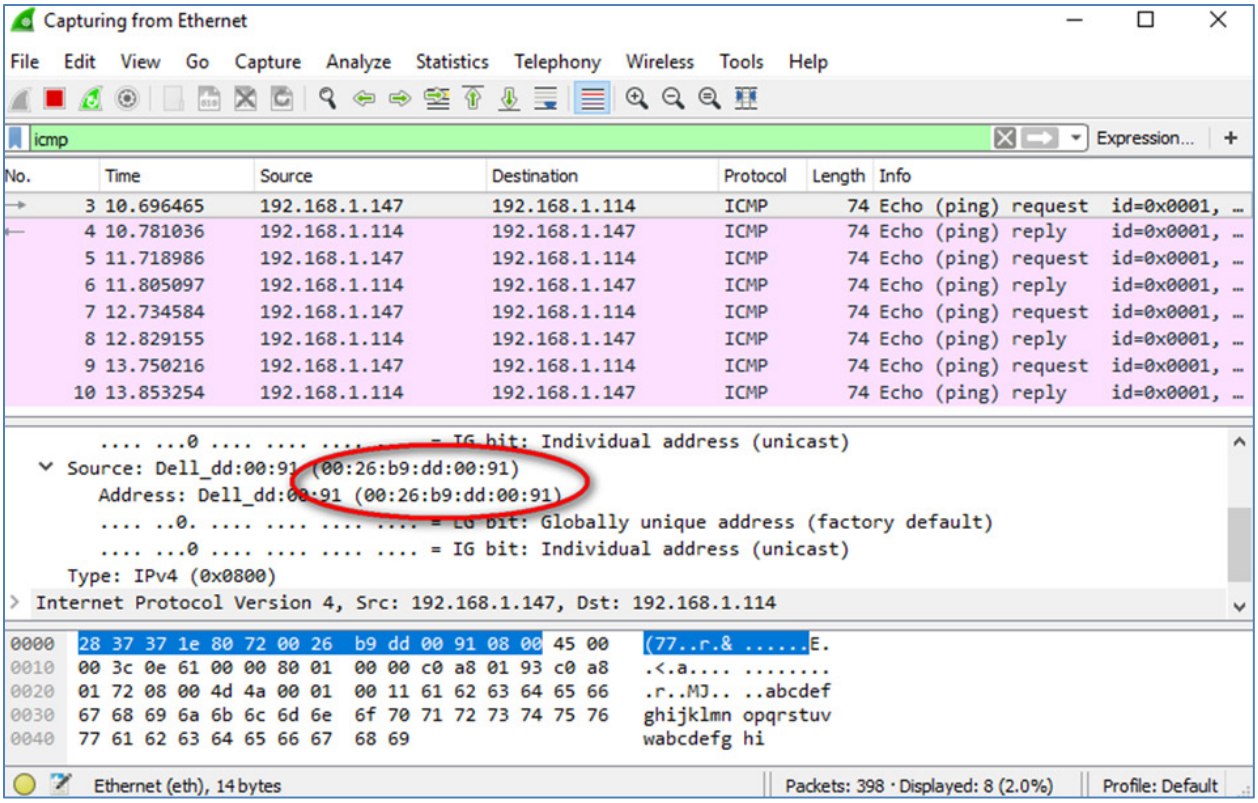
À l'étape 3, examinez les données qui ont été générées par les requêtes ping de l'ordinateur du membre de votre équipe. Les données Wireshark s'affichent dans trois sections : 1) la section supérieure affiche la liste des trames PDU capturées avec un résumé des informations de paquet IP, 2) la section 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 (notée à l'étape 1.b) ?

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

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

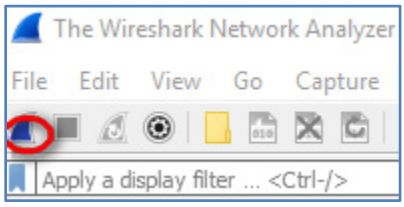
Remarque : dans l'exemple précédent d'une requête ICMP capturée, les données ICMP sont encapsulées dans une unité de données de protocole (PDU) de paquet IPv4 (en-tête IPv4) qui est ensuite encapsulée dans une PDU de trame Ethernet II (en-tête Ethernet II) en vue de sa transmission sur le réseau local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

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

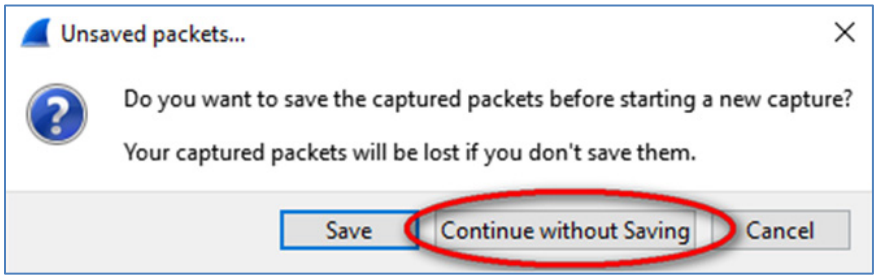
Dans la partie 2, vous enverrez des requêtes ping aux hôtes distants (les hôtes ne figurant pas sur le réseau local (LAN)) et vous examinerez les données générées à partir de ces requêtes ping. Ensuite, vous déterminerez en quoi ces données diffèrent des données examinées dans la partie 1.

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 :

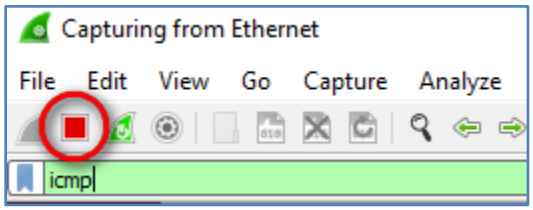
1) www.yahoo.com
2) www.cisco.com

3) www.google.com

```
C:\> ping www.yahoo.com

Pinging atsv2-fp.wg1.b.yahoo.com [98.139.180.180] with 32 bytes of data:
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=60ms TTL=53
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=42ms TTL=53

Ping statistics for 98.139.180.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 60ms, Average = 47ms

C:\> ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.13.155.188] with 32 bytes of data:
Reply from 23.13.155.188: bytes=32 time=20ms TTL=56
Reply from 23.13.155.188: bytes=32 time=21ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56

Ping statistics for 23.13.155.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 21ms, Average = 19ms

C:\> ping www.google.com

Pinging www.google.com [216.58.194.100] with 32 bytes of data:
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=55ms TTL=54
Reply from 216.58.194.100: bytes=32 time=57ms TTL=54

Ping statistics for 216.58.194.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 57ms, Average = 56ms

C:\>
```

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.

a. 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.

1er emplacement : IP : . . . MAC : : : : : :

2ème emplacement : IP : . . . MAC : : : : : :

3ème emplacement : IP : . . . MAC : : : : : :

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

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

Remarques générales

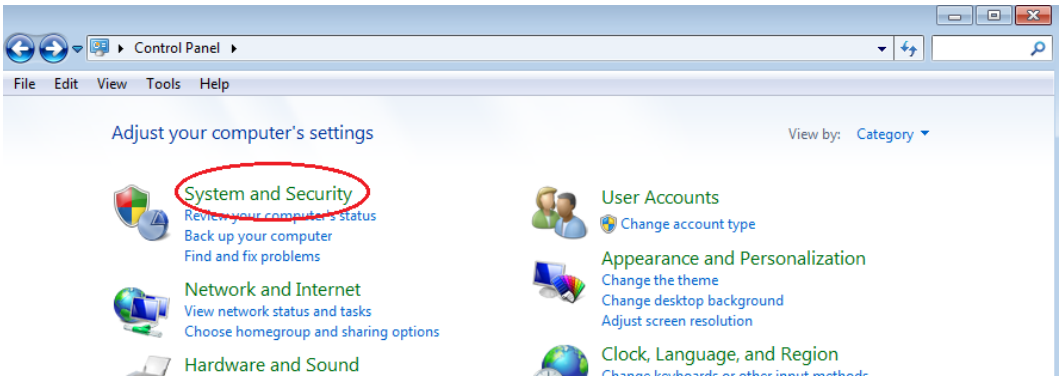
Pourquoi Wireshark affiche-t-il l'adresse MAC réelle des hôtes locaux, mais pas l'adresse MAC réelle des hôtes distants ?

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

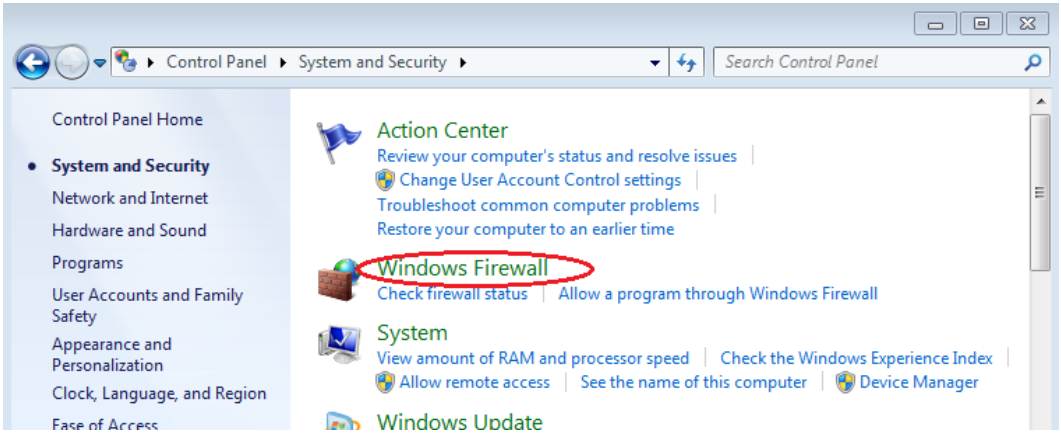
Si les membres de votre équipe ne parviennent pas à envoyer de requêtes ping à votre ordinateur, il est possible que votre pare-feu les bloque. Cette annexe explique comment créer une règle sur le pare-feu afin d'autoriser les requêtes ping. Elle décrit également comment désactiver la nouvelle règle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

Étape 3 : 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**.

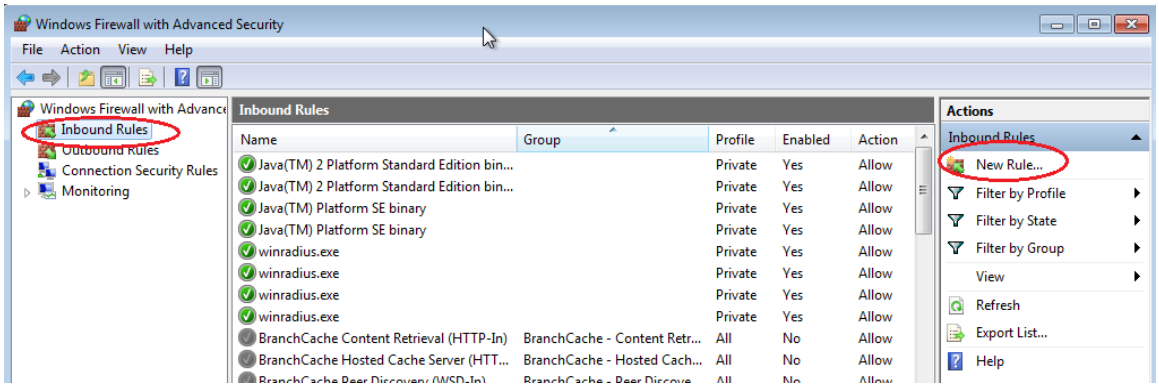


b. Dans la fenêtre **Système et sécurité**, cliquez sur **Pare-feu Windows**.

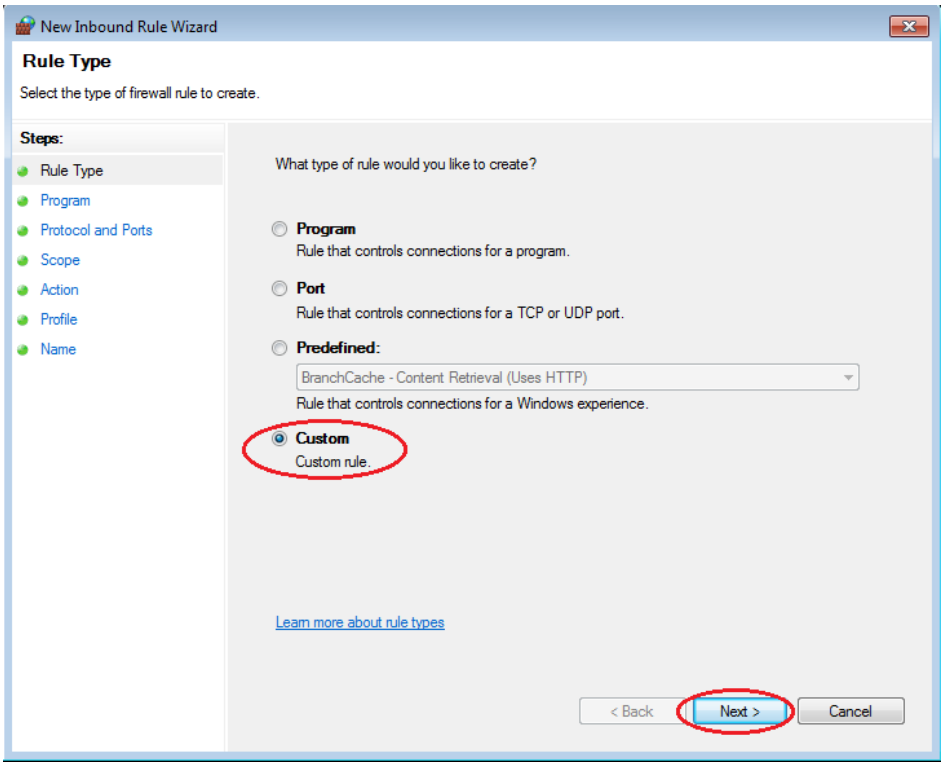


c. Dans le volet gauche de la fenêtre **Pare-feu Windows**, cliquez sur **Paramètres avancés**.

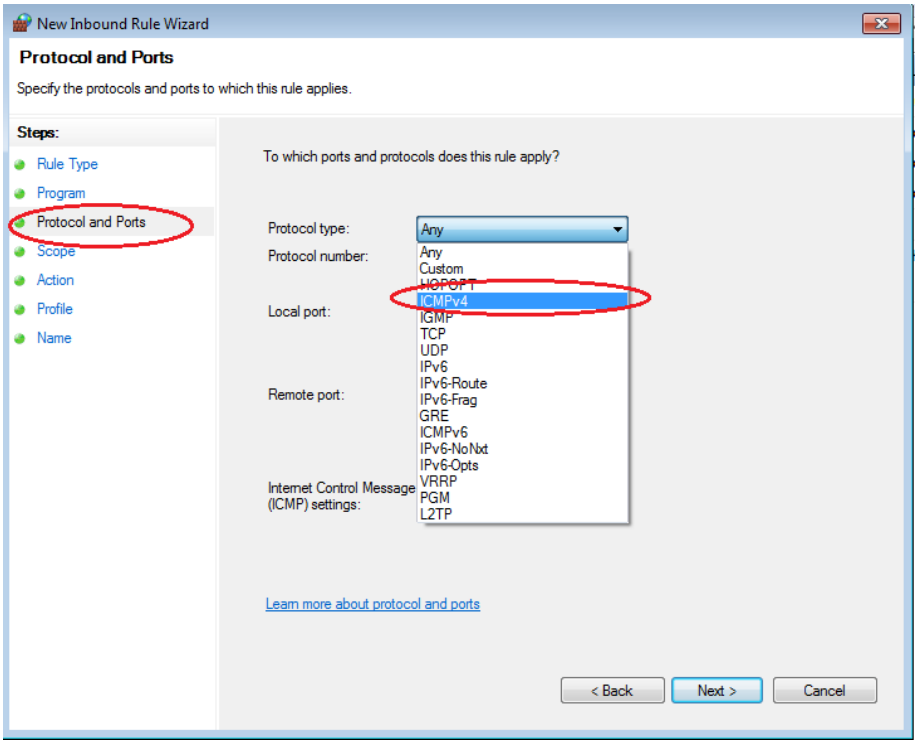
d. Dans la fenêtre des **fonctions de sécurité avancées**, choisissez l'option **Règles de trafic entrant** dans la barre latérale gauche, puis cliquez sur **Nouvelle règle…** dans la barre latérale droite.



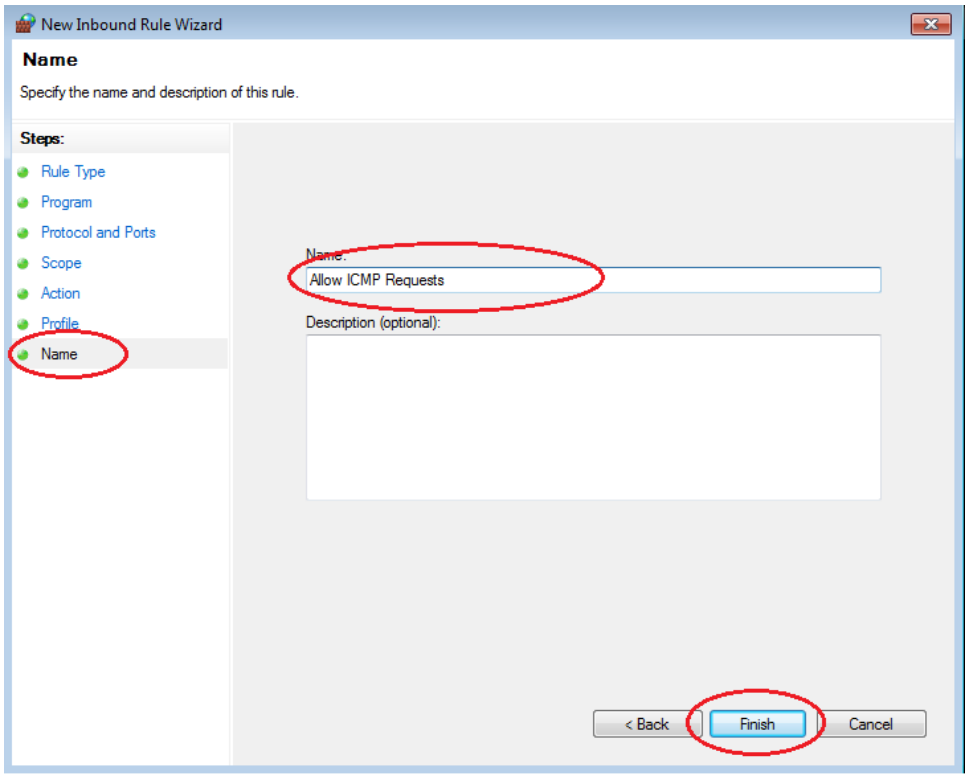
e. Cette action démarre l'Assistant **Nouvelle règle de trafic entrant**. Dans l'écran **Type de règle**, cliquez sur la case d'option **Personnalisée**, puis cliquez sur **Suivant**.



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. Dans le volet de gauche, cliquez sur l'option **Nom** et dans le champ **Nom**, tapez **Autoriser les demandes ICMP**. Cliquez sur **Terminer**.

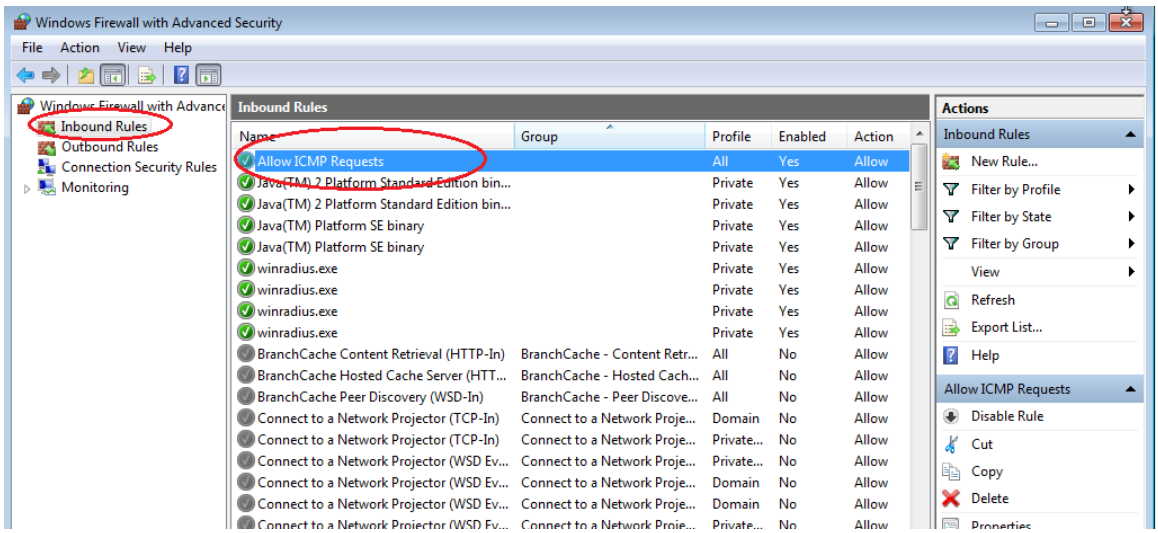


Cette nouvelle règle doit permettre aux membres de votre équipe de recevoir des réponses ping de votre ordinateur.

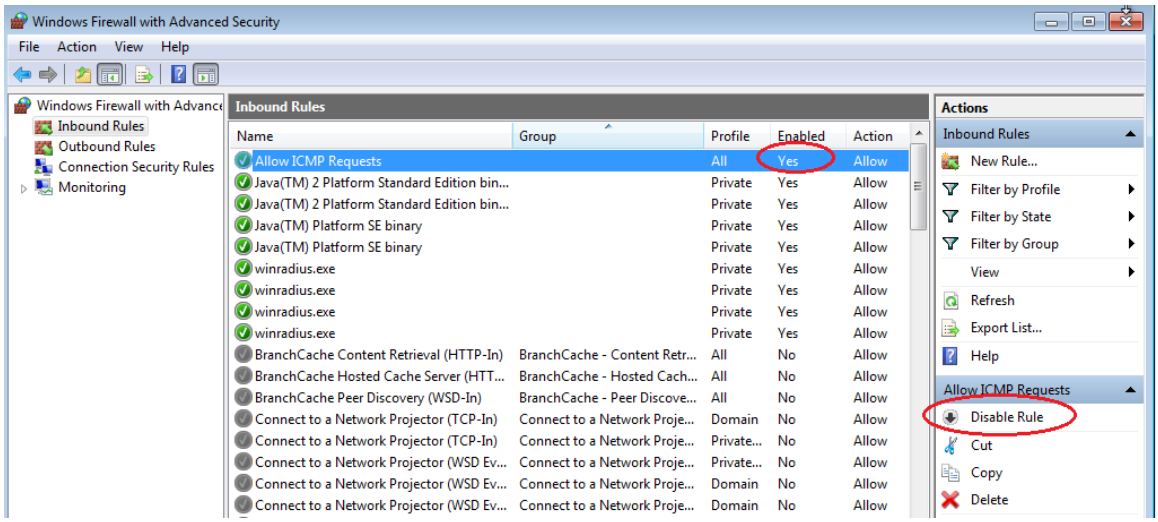
Étape 4 : Désactivation ou suppression de la nouvelle règle ICMP.

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'étape 1.



b. Pour désactiver la règle, cliquez sur l'option **Désactiver la règle**. Lorsque vous choisissez cette option, cette option devient **Activer la règle**. Vous pouvez basculer entre **Désactiver la règle** et **Activer la règle**. Le statut de la règle s'affiche également dans la colonne **Activée** de la liste **Règles de trafic entrant**.



c. Pour supprimer définitivement la règle ICMP, cliquez sur **Supprimer**. Si vous choisissez cette option, vous devez recréer la règle pour autoriser les réponses ICMP.