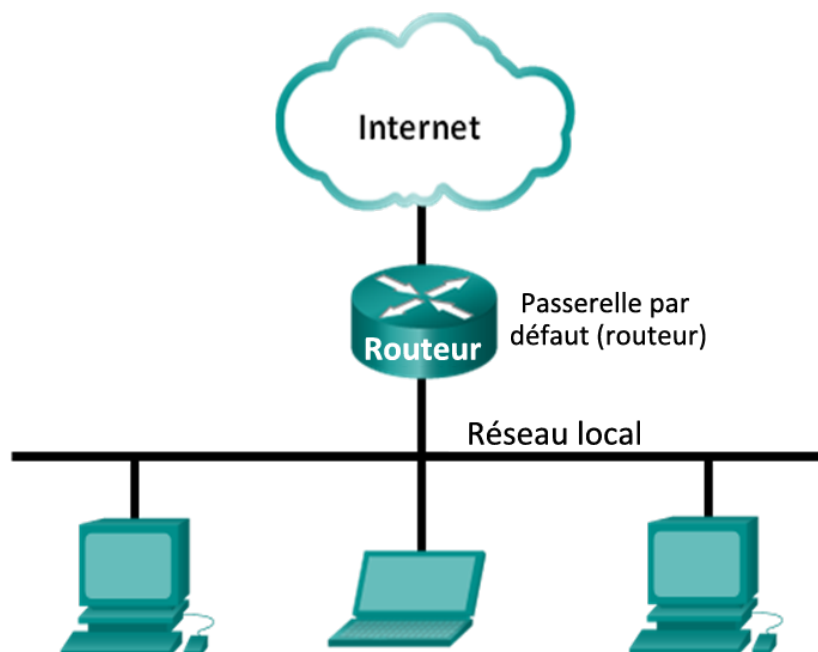


Travaux pratiques - Utilisation de Wireshark pour voir le trafic réseau

Topologie



Objectifs

1ère partie : Télécharger et installer Wireshark (facultatif)

2e partie : Capturer et analyser les données ICMP locales avec Wireshark

- Démarrez et arrêtez la capture des données du trafic de la commande ping vers les hôtes locaux.
- Trouvez les informations relatives à l'adresse IP et à l'adresse MAC dans les unités de données de protocole capturées.

3e partie : Capturer et analyser les données ICMP distantes avec Wireshark

- Démarrez et arrêtez la capture des données du trafic de la commande ping vers les hôtes distants.
- Trouvez les informations relatives à l'adresse IP et à l'adresse MAC dans les unités de données de protocole capturées.
- Expliquez pourquoi les adresses MAC des hôtes distants sont différentes des adresses MAC des hôtes locaux.

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 PDU des flux de données circulant du réseau. Il permet de décoder et d'analyser leur contenu conformément aux spécifications RFC ou autres appropriées.

Wireshark est un outil 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. Ces travaux pratiques contiennent des instructions permettant de télécharger et d'installer Wireshark, bien qu'il puisse être déjà installé. Au cours de ces travaux pratiques, vous utiliserez Wireshark pour capturer les adresses IP des paquets ICMP et les adresses MAC de trames Ethernet.

Ressources requises

- 1 ordinateur (Windows 7, Vista ou XP, équipé d'un accès à Internet)
- Des ordinateurs supplémentaires sur un réseau local (LAN) seront utilisés pour répondre aux requêtes ping.

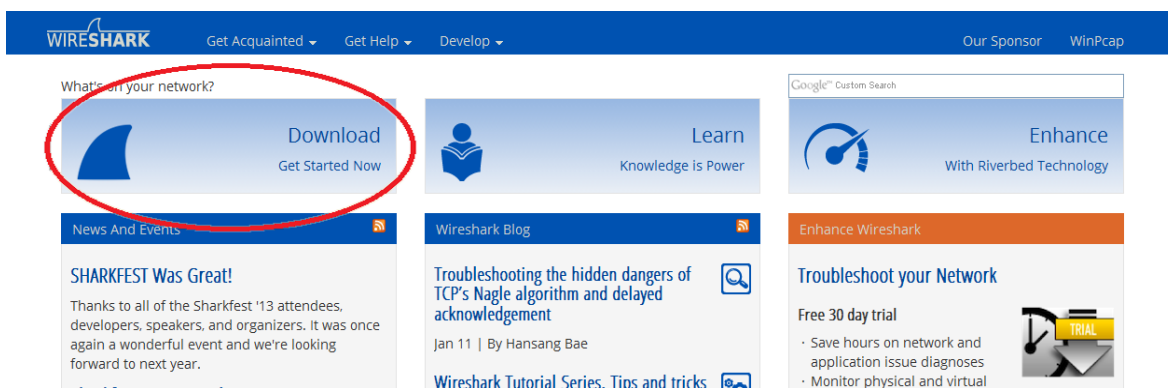
1ère partie : Télécharger et installer Wireshark (facultatif)

Wireshark est devenu le programme standard d'analyse de paquets pour les ingénieurs réseau. Ce logiciel gratuit ouvert est disponible pour de nombreux systèmes d'exploitation différents, y compris Windows, Mac et Linux. Dans la première partie de ces travaux pratiques, vous téléchargerez et installerez le logiciel Wireshark sur votre ordinateur.

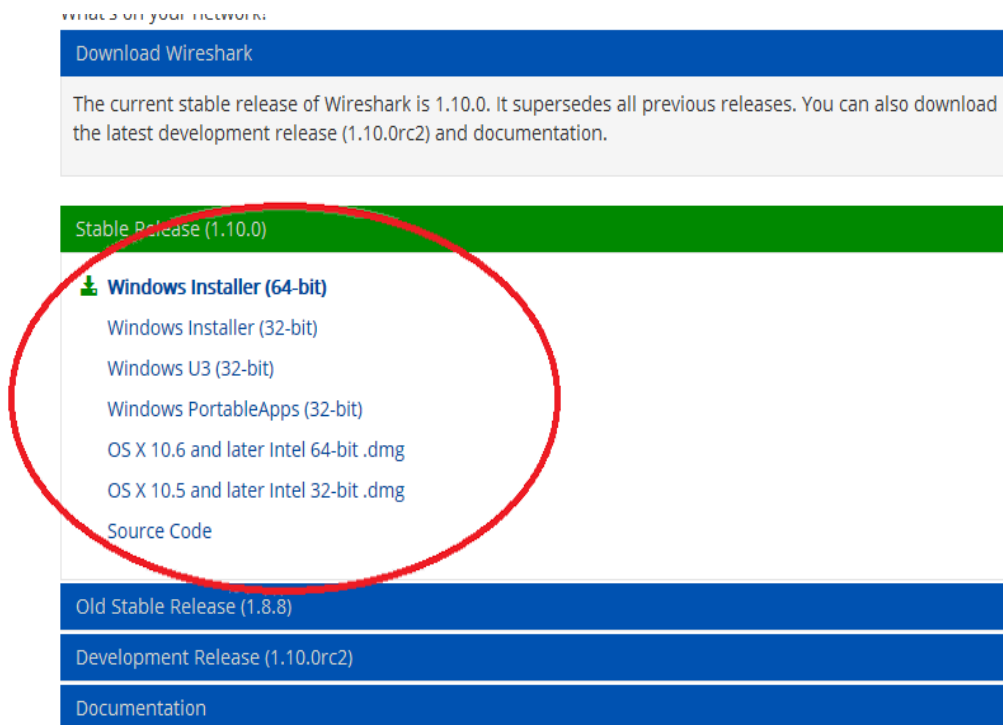
Remarque : si Wireshark est déjà installé sur votre ordinateur, vous pouvez ignorer la première partie et accéder directement à la deuxième partie. Si Wireshark n'est pas installé sur votre ordinateur, vérifiez auprès de votre instructeur quelle est la stratégie de téléchargement des logiciels de votre école.

Étape 1 : Téléchargez Wireshark.

- Wireshark peut être téléchargé à partir de www.wireshark.org.
- Cliquez sur **Download Wireshark (Télécharger Wireshark)**.



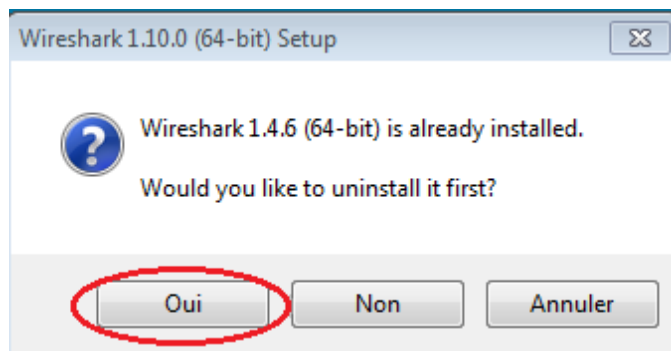
- c. Sélectionnez la version de logiciel dont vous avez besoin en fonction de l'architecture et du système d'exploitation de votre ordinateur. Par exemple, si vous disposez d'un ordinateur 64 bits exécutant Windows, choisissez **Windows Installer (64-bit) (Programme d'installation de Windows (64 bits))**.



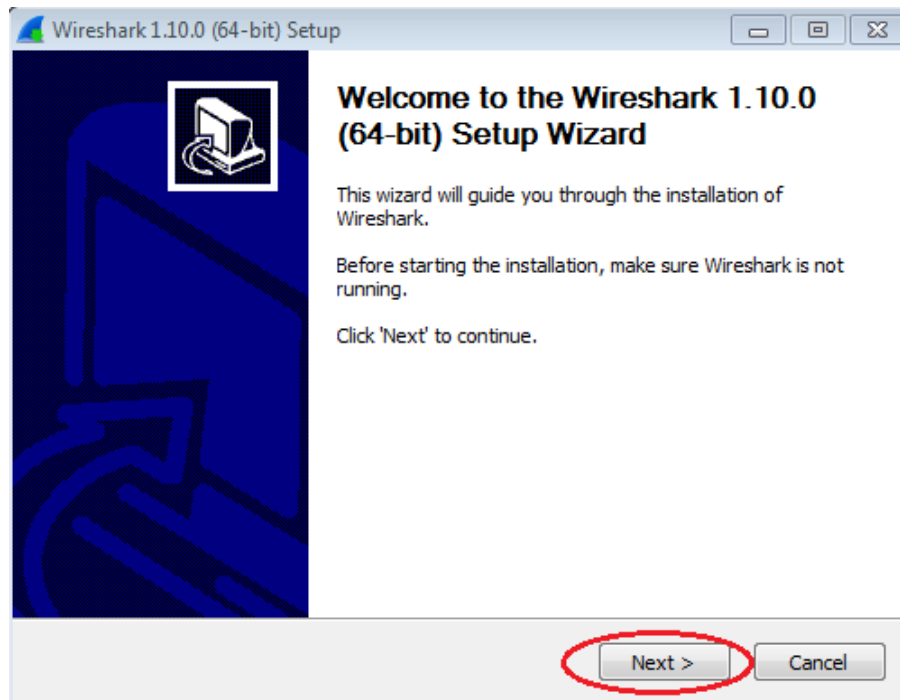
Une fois que vous avez effectué votre sélection, le téléchargement devrait commencer. L'emplacement du fichier téléchargé dépend de votre navigateur et du système d'exploitation que vous utilisez. Pour les utilisateurs Windows, l'emplacement par défaut est le dossier **Downloads**.

Étape 2 : Installez Wireshark.

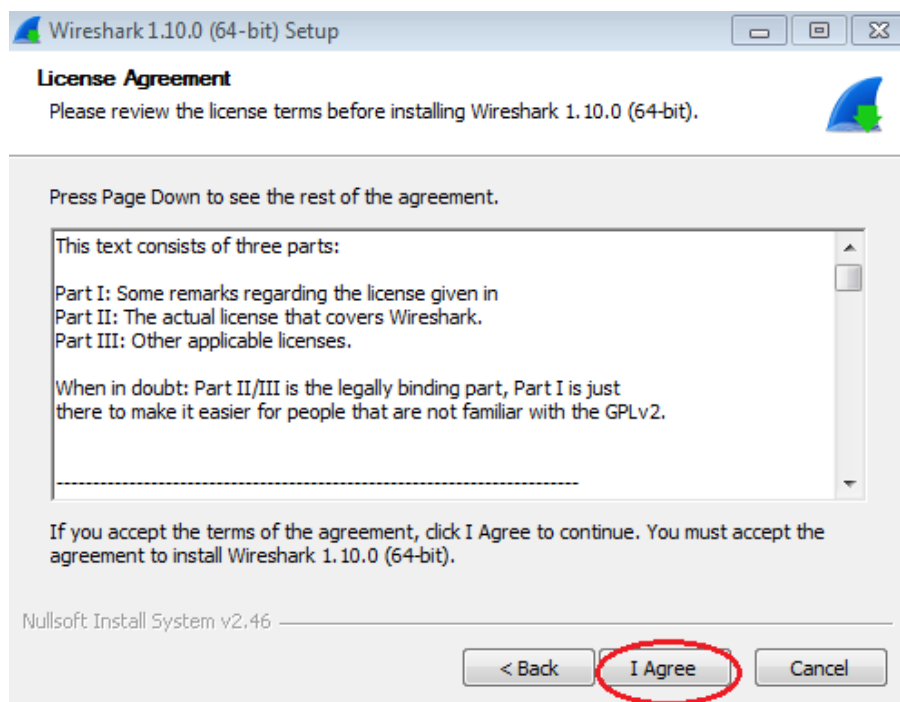
- a. Le fichier téléchargé est nommé **Wireshark-win64-x.x.x.exe**, où **x** représente le numéro de version. Double-cliquez sur le fichier pour lancer la procédure d'installation.
- b. Répondez à tous les messages de sécurité qui s'affichent à l'écran. Si vous disposez déjà d'une copie de Wireshark sur votre ordinateur, vous serez invité à désinstaller l'ancienne version avant d'installer la nouvelle version. Nous vous recommandons de supprimer l'ancienne version de Wireshark avant d'installer une autre version. Cliquez sur **Oui** pour désinstaller la version précédente de Wireshark.



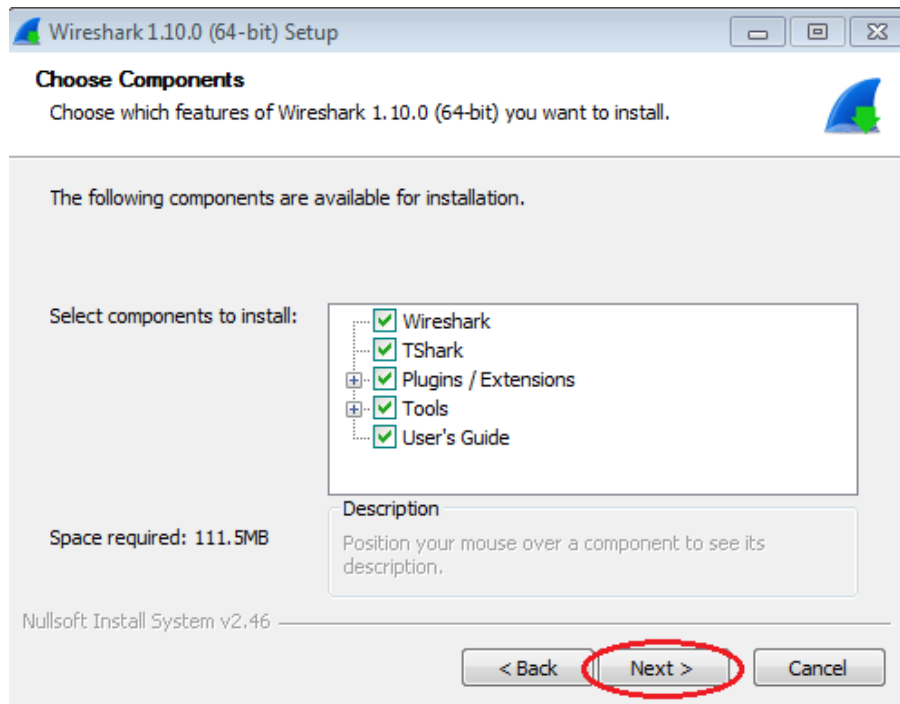
- c. Si c'est la première fois que vous installez Wireshark, ou après avoir terminé la procédure de désinstallation, accédez à l'assistant de configuration de Wireshark. Cliquez sur **Next (Suivant)**.



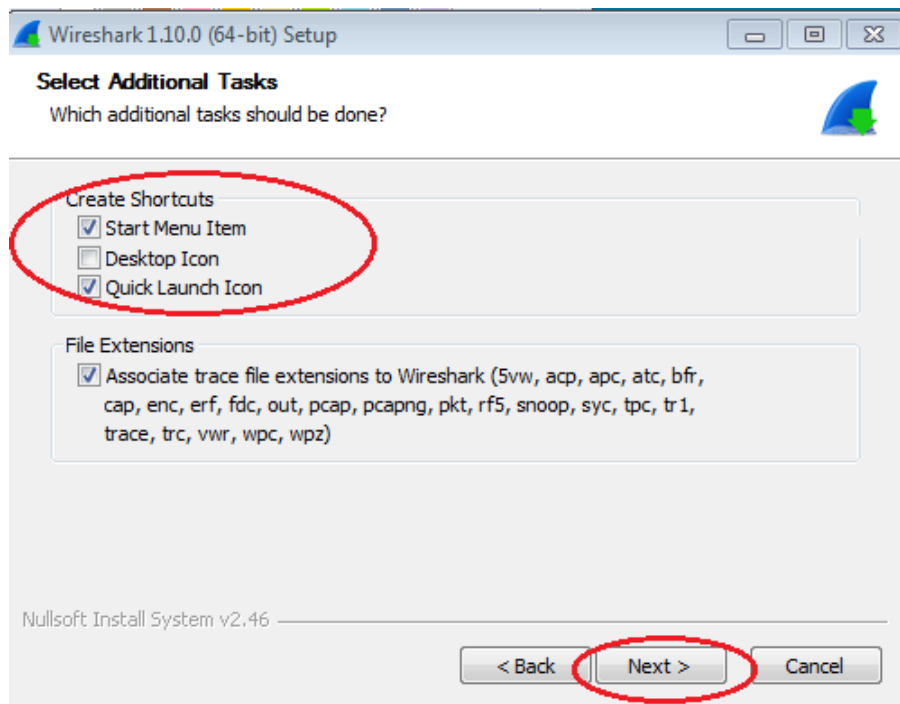
- d. Continuez à avancer dans la procédure d'installation. Cliquez sur **I agree (J'accepte)** lorsque la fenêtre contenant l'accord de licence s'affiche.



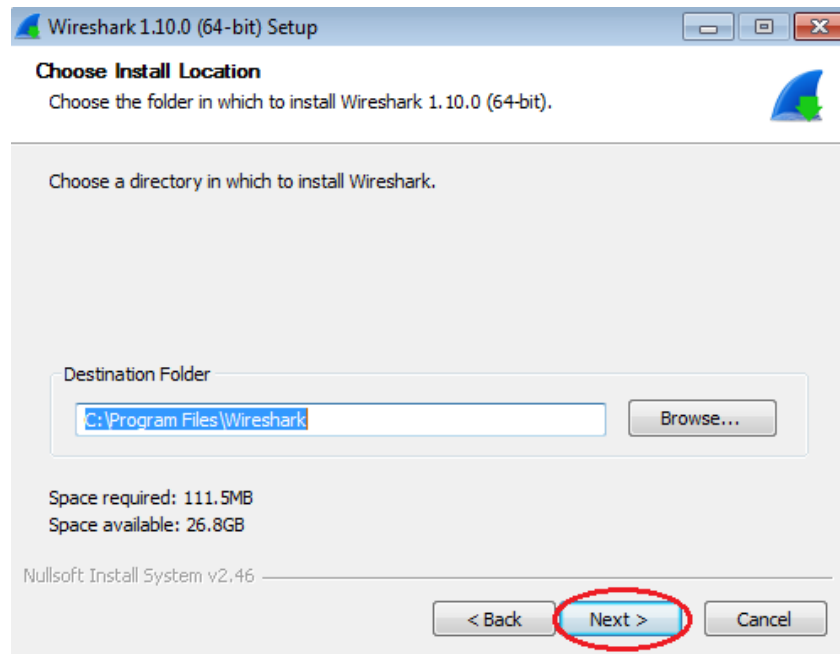
- e. Conservez les paramètres par défaut dans la fenêtre Choose Components (Choisir les composants) et cliquez sur **Next (Suivant)**.



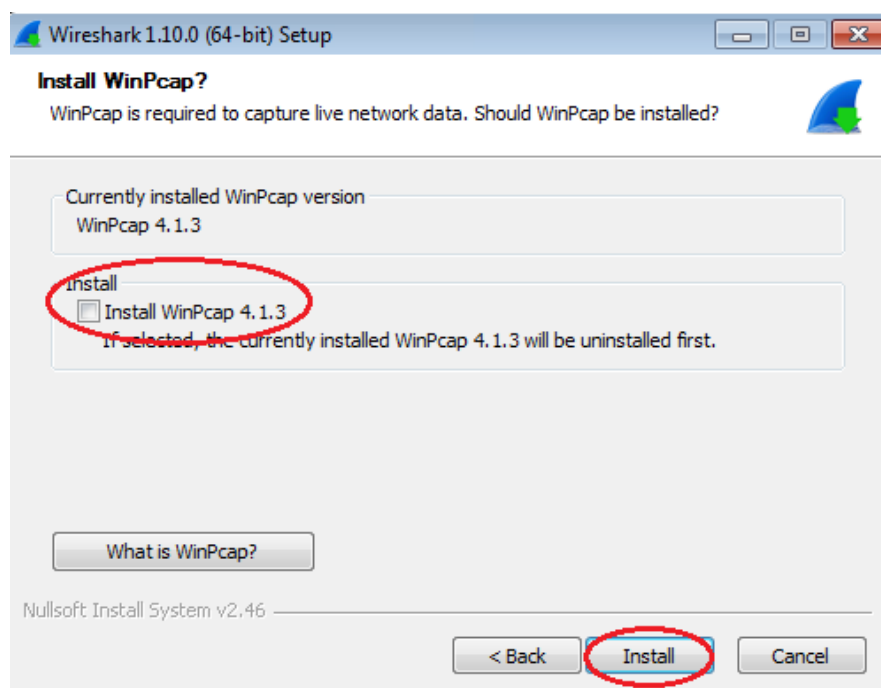
- f. Choisissez les options de raccourci souhaitées et cliquez sur **Next (Suivant)**.



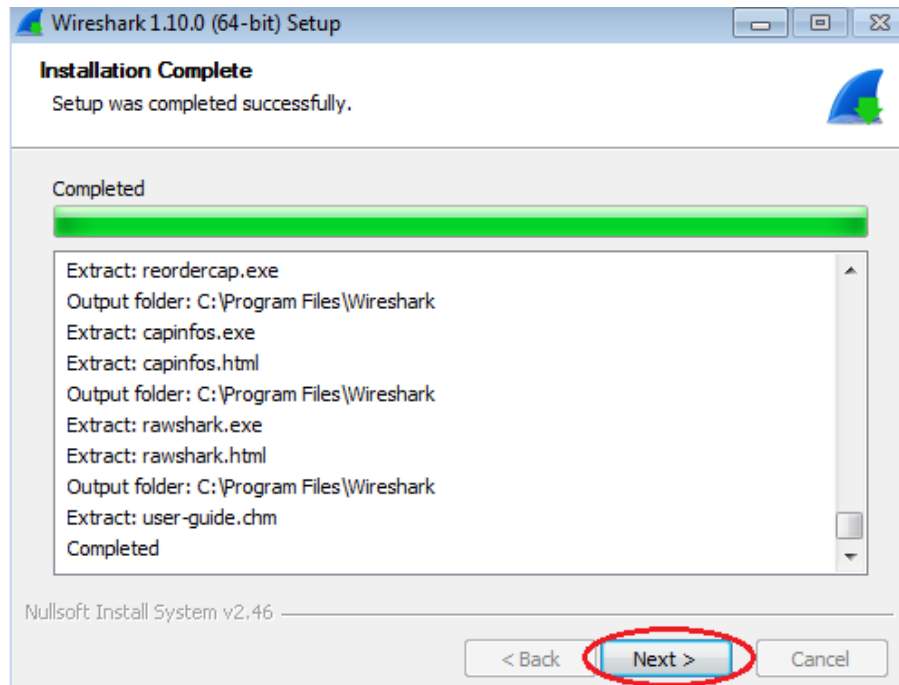
- g. Vous pouvez modifier l'emplacement d'installation de Wireshark, mais sauf si vous disposez d'un espace disque limité, nous vous recommandons de conserver l'emplacement par défaut.



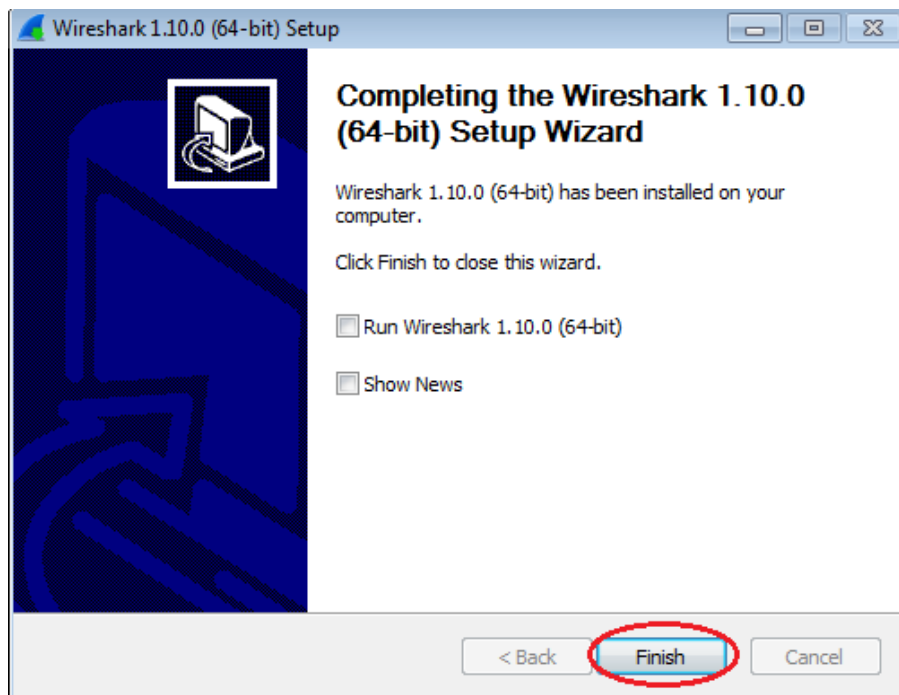
- h. Pour enregistrer des données réseau réelles, WinPcap doit être installé sur votre ordinateur. Si WinPcap est déjà installé sur votre ordinateur, la case à cocher Install (Installer) sera désactivée. Si la version de WinPcap que vous avez installée est antérieure à la version fournie avec Wireshark, il est recommandé d'autoriser l'installation de la version la plus récente en activant la case à cocher **Install WinPcap x.x.x** (numéro de version) (Installer WinPcap).
- i. Finalisez l'installation au moyen de l'Assistant si vous installez WinPcap.



- j. Wireshark commence à installer ses fichiers et affiche une fenêtre distincte avec l'état de l'installation. Cliquez sur **Next (Suivant)** une fois l'installation terminée.



- k. Cliquez sur **Finish (Terminer)** pour terminer le processus d'installation de Wireshark .



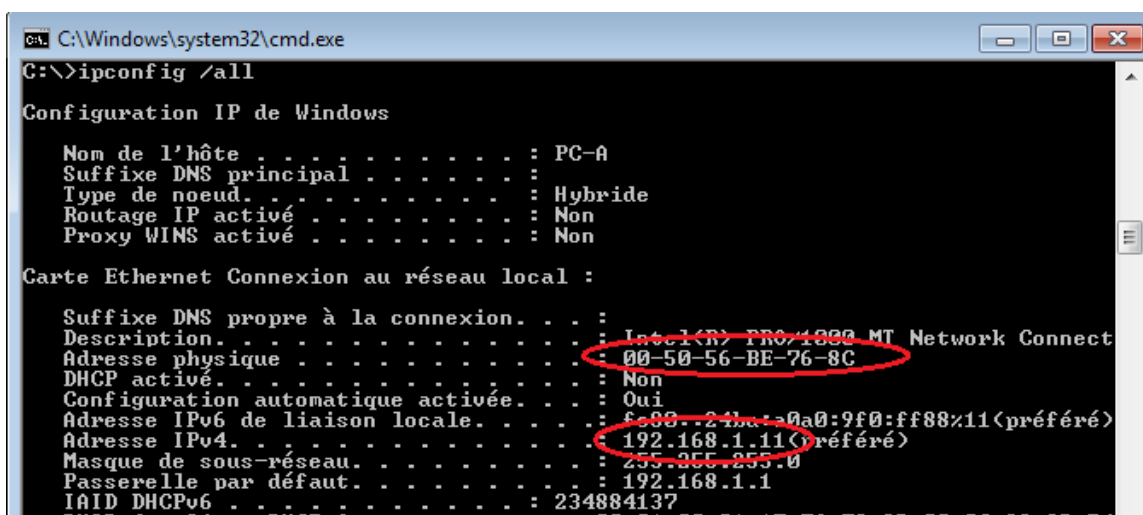
2e partie : Capturer et analyser les données ICMP locales avec Wireshark

Dans la deuxième partie 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.

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



```
C:\Windows\system32\cmd.exe
G:\>ipconfig /all

Configuration IP de Windows

Nom de l'hôte . . . . . : PC-A
Suffixe DNS principal . . . . . :
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non

Carte Ethernet Connexion au réseau local :

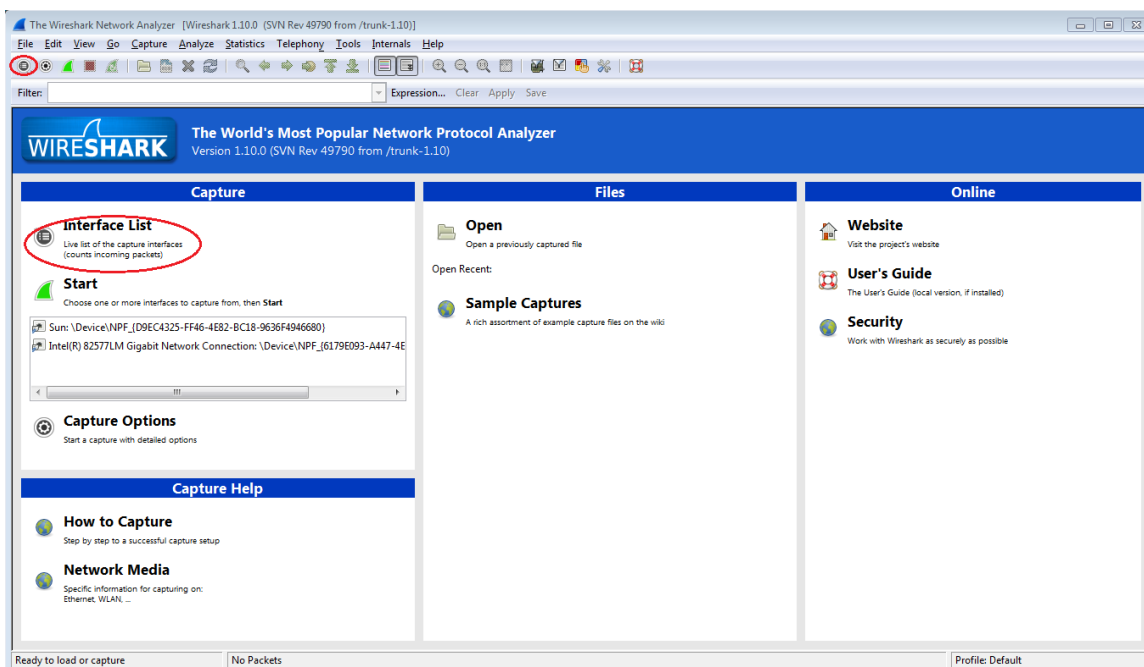
Suffixe DNS propre à la connexion. . . :
Description. . . . . : Intel(R) PRO/1000 MT Network Connect
Adresse physique . . . . . : 00-50-56-BE-76-8C
DHCP activé . . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::21ba:a0a0:9f0:ff88%11(préfé
Adresse IPv4. . . . . : 192.168.1.11(Préfé
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.1.1
IAD DHCPv6 . . . . . : 234884137
DUID de liaison DHCPv6 . . . . . : 00-01-00-01-17-8C-72-3D-00-0C-20-0D-F4
```

- Demandez à un membre de l'équipe de fournir l'adresse IP de son ordinateur et donnez-lui 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.

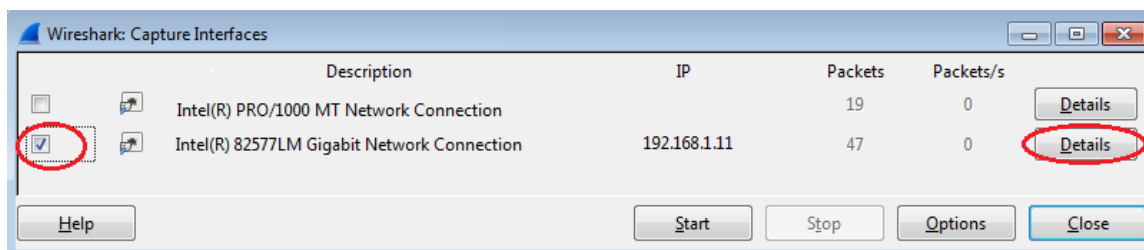
- Sur votre ordinateur, cliquez sur le bouton **Démarrer** pour voir s'afficher Wireshark en tant que l'un des programmes du menu contextuel. Double-cliquez sur **Wireshark**.

- b. Une fois que Wireshark démarre, cliquez sur **Interface List**.

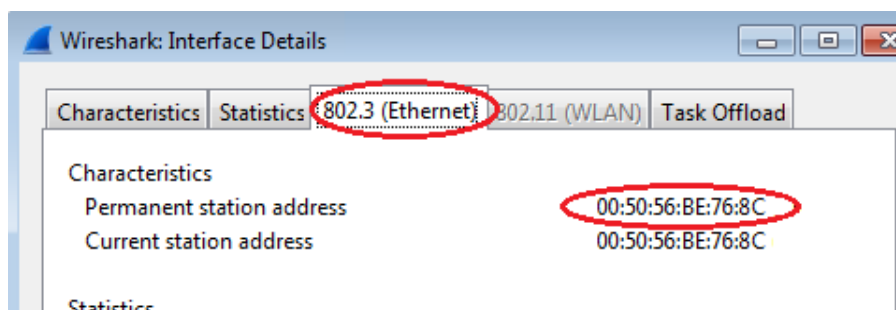


Remarque : cliquer sur la première icône d'interface dans la barre d'icônes permet également d'ouvrir la liste d'interfaces.

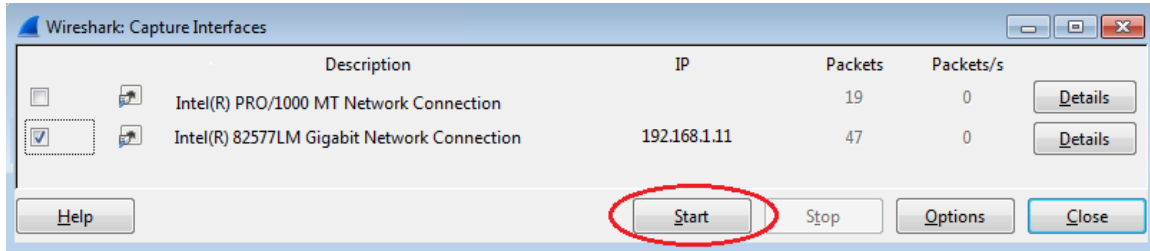
- c. Dans la fenêtre Wireshark : Capture Interfaces (Wireshark : interfaces de capture), activez la case à cocher en regard de l'interface connectée à votre réseau local (LAN).



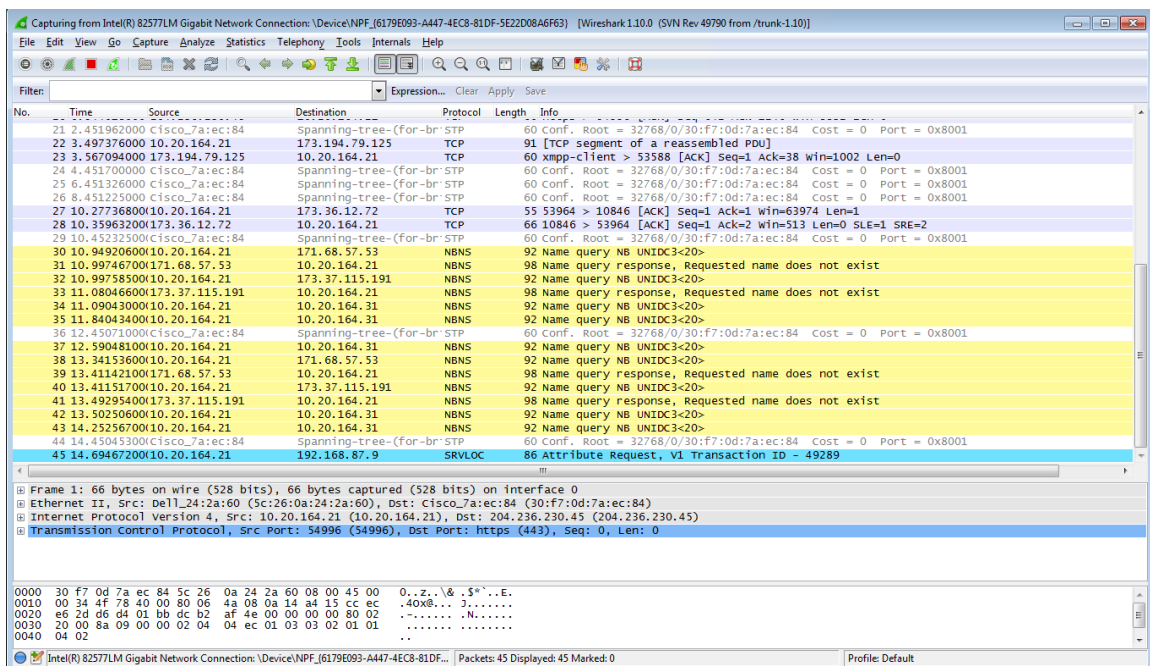
Remarque : si plusieurs interfaces sont listées et que vous ne savez pas quelle interface vérifier, cliquez sur le bouton **Details (Détails)**, puis cliquez sur l'onglet **802.3 (Ethernet)**. Vérifiez que l'adresse MAC correspond à ce que vous avez noté à l'étape 1b. Fermez la fenêtre de Interface Details (Détails d'interface) après avoir vérifié l'interface appropriée.



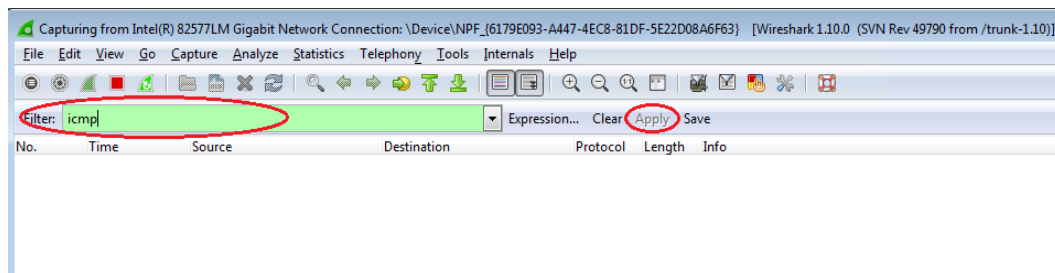
- d. Après avoir vérifié l'interface appropriée, cliquez sur **Start (Démarrer)** pour démarrer la capture des données.



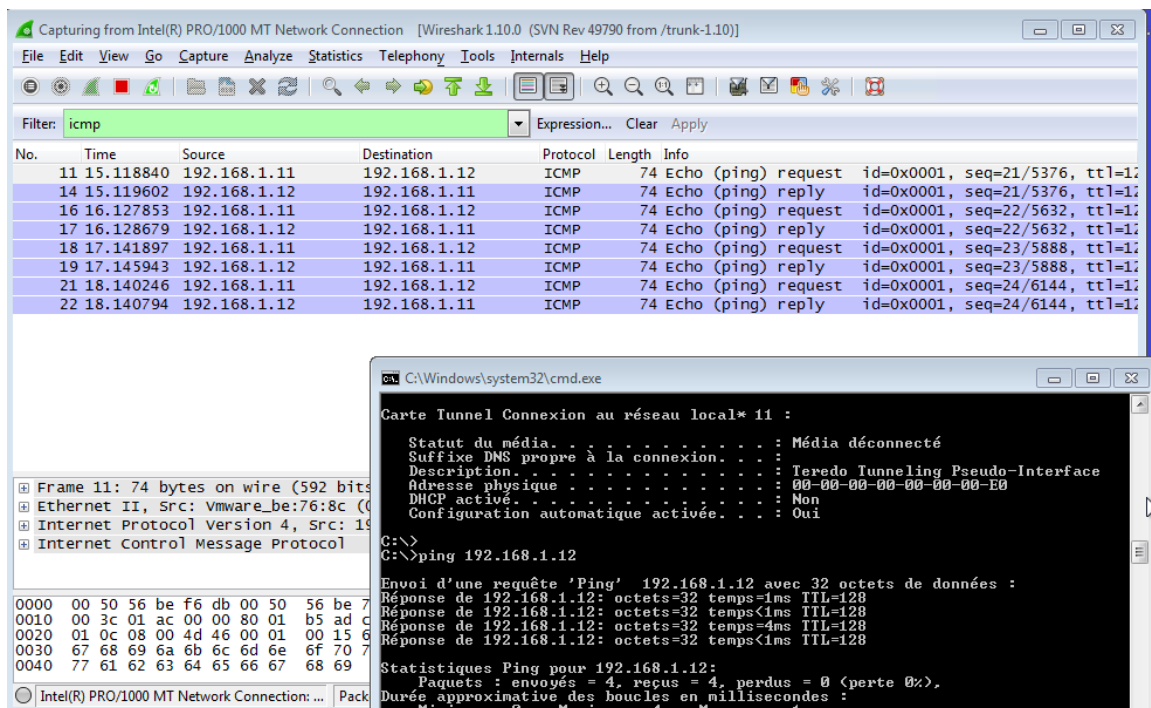
Les informations commencent à défiler vers le bas à partir de la section supérieure dans Wireshark. Les lignes de données s'affichent en différentes couleurs selon le protocole.



- 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 qui sont 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 (Filtre) en haut de Wireshark et appuyez sur Entrée ou cliquez sur le bouton **Apply (Appliquer)** pour afficher uniquement les unités de données de protocole (PDU) (ping) ICMP.

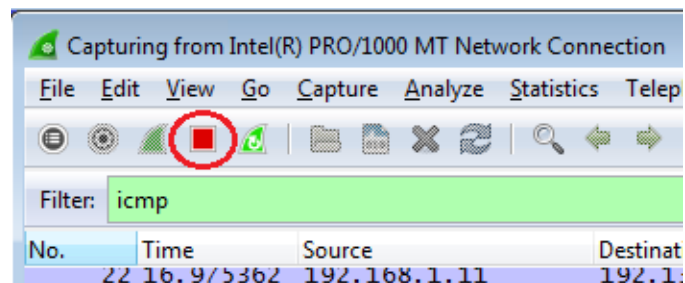


- f. Ce filtre fait disparaître toutes les données dans la fenêtre du haut, mais la capture du trafic de l'interface se poursuit toujours. Affichez la fenêtre d'invite de commandes que vous avez ouverte précédemment et envoyez une requête ping à l'adresse IP que vous avez reçue du membre de votre équipe.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



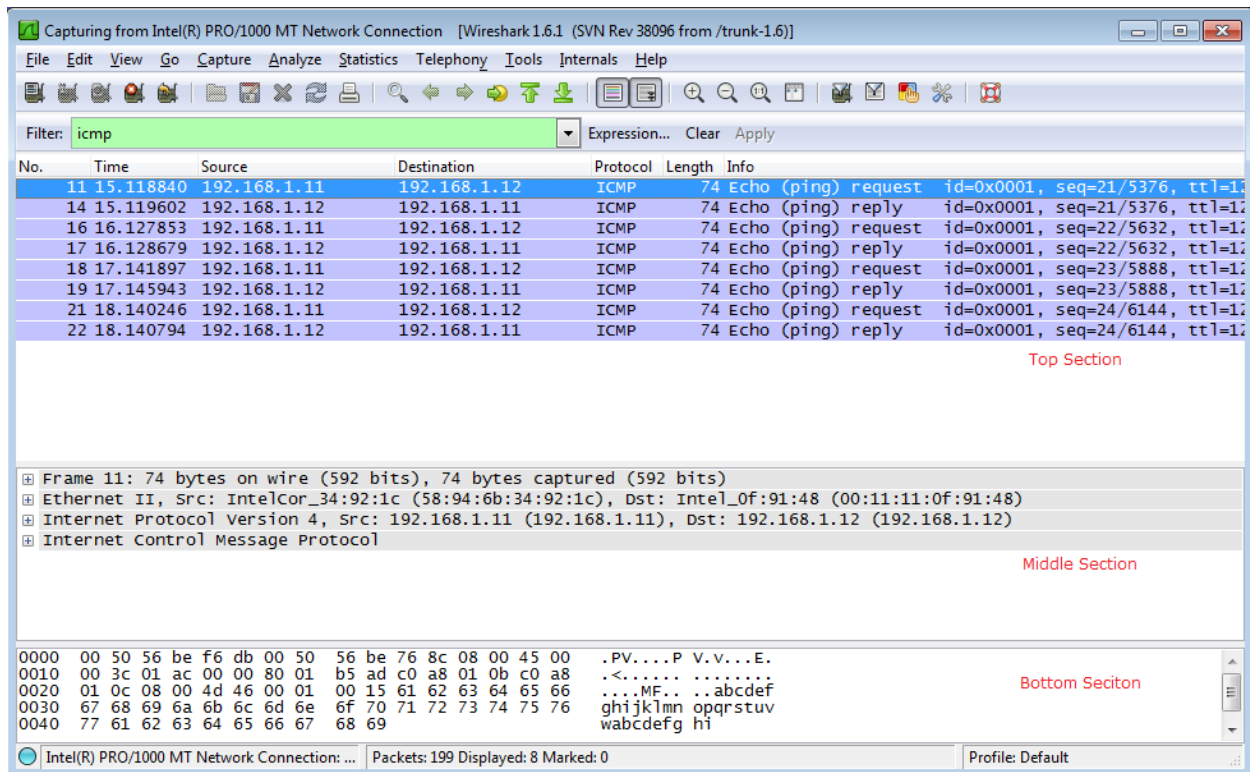
Remarque : si l'ordinateur du membre de votre équipe ne répond pas à vos requêtes ping, c'est peut-être parce que le pare-feu de son ordinateur bloque ces requêtes. Consultez l'Appendix A: Allowing ICMP Traffic Through a Firewall pour savoir comment autoriser le trafic ICMP via le pare-feu sous Windows 7.

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

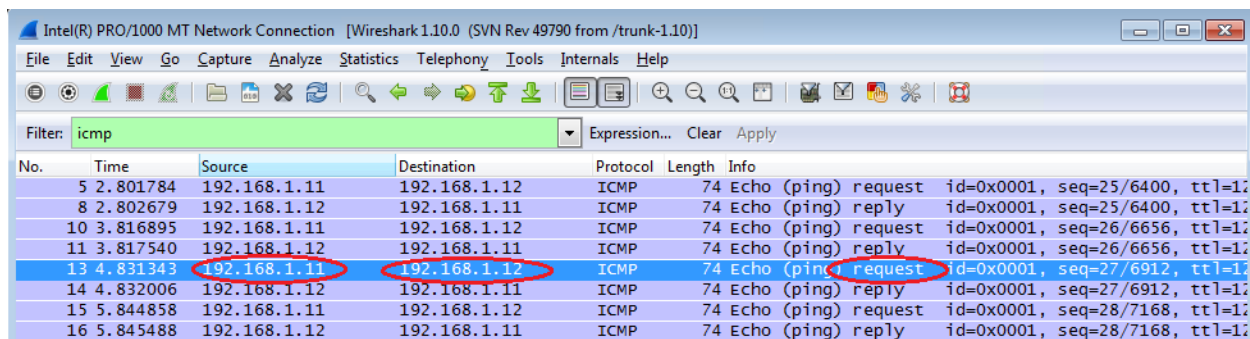


Étape 3 : Examinez les données capturées.

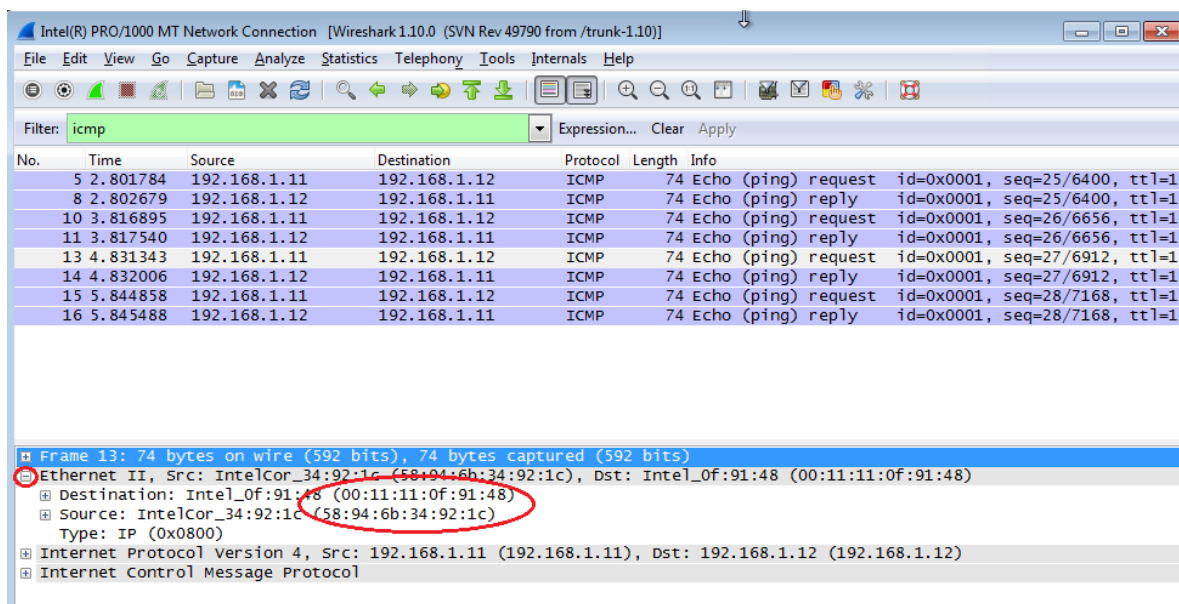
À l'étape 3, examinez les données qui ont été générées par les requêtes ping de l'ordinateur du membre de votre équipe. Les données Wireshark s'affichent dans trois sections : 1) la section supérieure affiche la liste des trames PDU capturées avec un résumé des informations de paquet IP, 2) la section centrale liste les informations PDU correspondant à la trame sélectionnée dans la partie supérieure de l'écran et sépare une trame capturée PDU par 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.



- 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. Cette trame PDU étant toujours sélectionnée dans la partie supérieure, accédez à la section centrale. Cliquez sur le signe plus à gauche de la ligne Ethernet II pour afficher les adresses MAC de la destination et de la source.



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

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

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

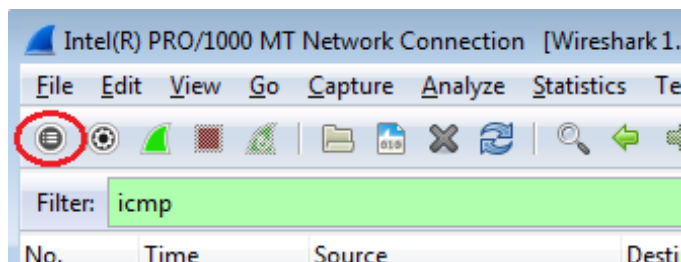
Remarque : dans l'exemple précédent d'une requête ICMP capturée, les données ICMP sont encapsulées dans une unité de données de protocole (PDU) d'un paquet IPv4 (en-tête IPv4) qui est ensuite encapsulée dans une PDU de trame Ethernet II (en-tête Ethernet II) en vue de sa transmission du réseau local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

3e partie : Capturer et analyser les données ICMP locales dans Wireshark

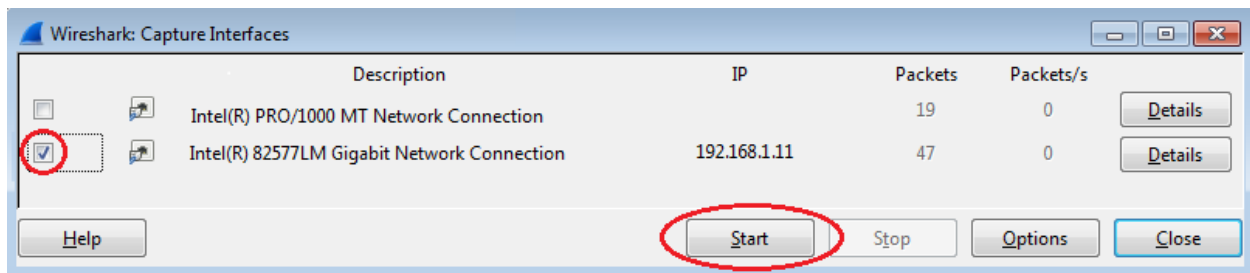
Dans cette troisième partie, vous enverrez des requêtes ping aux hôtes distants (les hôtes ne figurant pas du réseau local (LAN)) et vous examinerez les données générées à partir de ces requêtes ping. Ensuite, vous déterminerez en quoi ces données diffèrent des données examinées dans la deuxième partie.

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

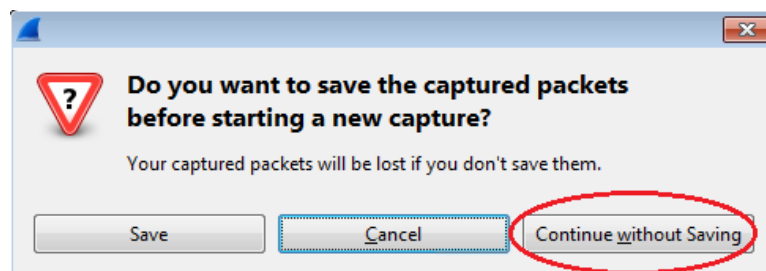
- a. Cliquez sur l'icône **Interface List (Liste d'interfaces)** pour afficher la liste des interfaces d'ordinateur.



- b. Vérifiez que la case à cocher en regard de l'interface LAN est activée, puis cliquez sur **Start (Démarrer)**.



- c. 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)**.



d. 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:\Windows\system32\cmd.exe

C:\>ping www.yahoo.com

Envoi d'une requête 'ping' sur www.yahoo.com [72.30.38.140] avec 32 octets de données :
Réponse de 72.30.38.140: octets=32 temps=1ms TTL=255
Réponse de 72.30.38.140: octets=32 temps<1ms TTL=255
Réponse de 72.30.38.140: octets=32 temps<1ms TTL=255
Réponse de 72.30.38.140: octets=32 temps<1ms TTL=255

Statistiques Ping pour 72.30.38.140:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\>ping www.cisco.com

Envoi d'une requête 'ping' sur www.cisco.com [198.133.219.25] avec 32 octets de données :
Réponse de 198.133.219.25: octets=32 temps<1ms TTL=255
Réponse de 198.133.219.25: octets=32 temps<1ms TTL=255
Réponse de 198.133.219.25: octets=32 temps<1ms TTL=255
Réponse de 198.133.219.25: octets=32 temps<1ms TTL=255

Statistiques Ping pour 198.133.219.25:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\>ping www.google.com

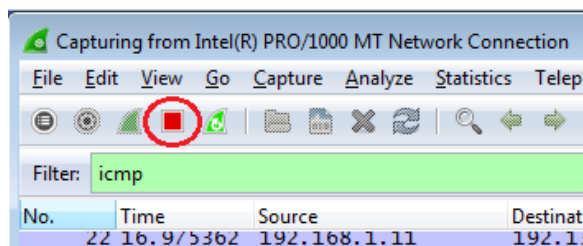
Envoi d'une requête 'ping' sur www.google.com [74.125.129.99] avec 32 octets de données :
Réponse de 74.125.129.99: octets=32 temps=1ms TTL=255
Réponse de 74.125.129.99: octets=32 temps<1ms TTL=255
Réponse de 74.125.129.99: octets=32 temps<1ms TTL=255
Réponse de 74.125.129.99: octets=32 temps<1ms TTL=255

Statistiques Ping pour 74.125.129.99:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

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.

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



Étape 2 : Examen et analyse des données à partir 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.

- 1^{er} emplacement : IP : _____ MAC : _____
- 2^e emplacement : IP : _____ MAC : _____
- 3^e emplacement : IP : _____ MAC : _____

b. Quel élément important tirez-vous de ces informations ?

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

Remarques générales

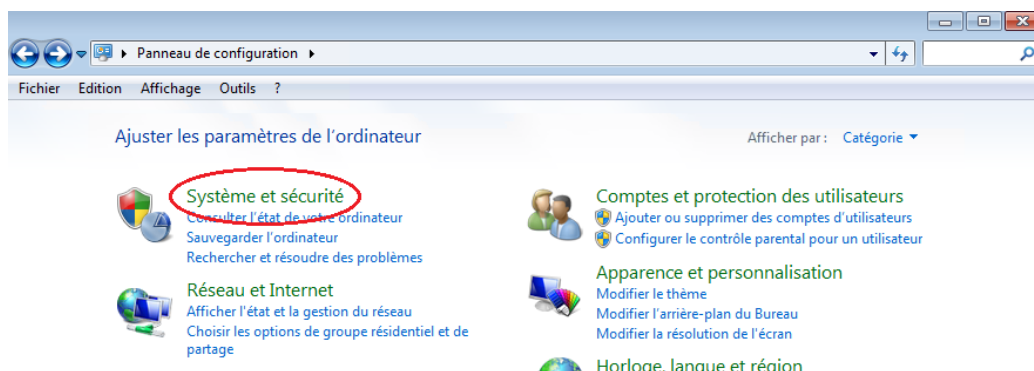
Pourquoi Wireshark affiche-t-il l'adresse MAC réelle des hôtes locaux, mais pas l'adresse MAC réelle des hôtes distants ?

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

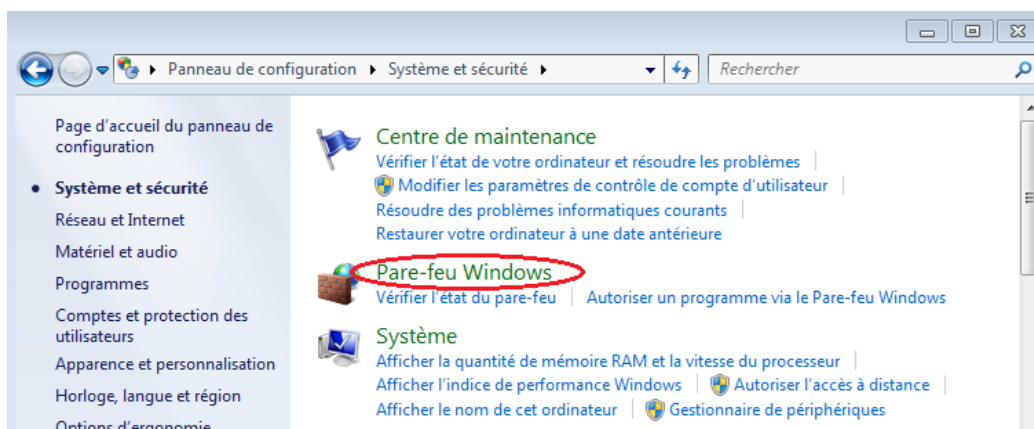
Si les membres de votre équipe ne parviennent pas à envoyer des requêtes ping à votre ordinateur, c'est peut-être parce que le pare-feu bloque ces demandes. Cette annexe explique comment créer une règle sur le pare-feu afin d'autoriser les requêtes ping. Elle décrit également comment désactiver la nouvelle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

Étape 1 : Créez une règle d'accès autorisant le trafic ICMP via le pare-feu.

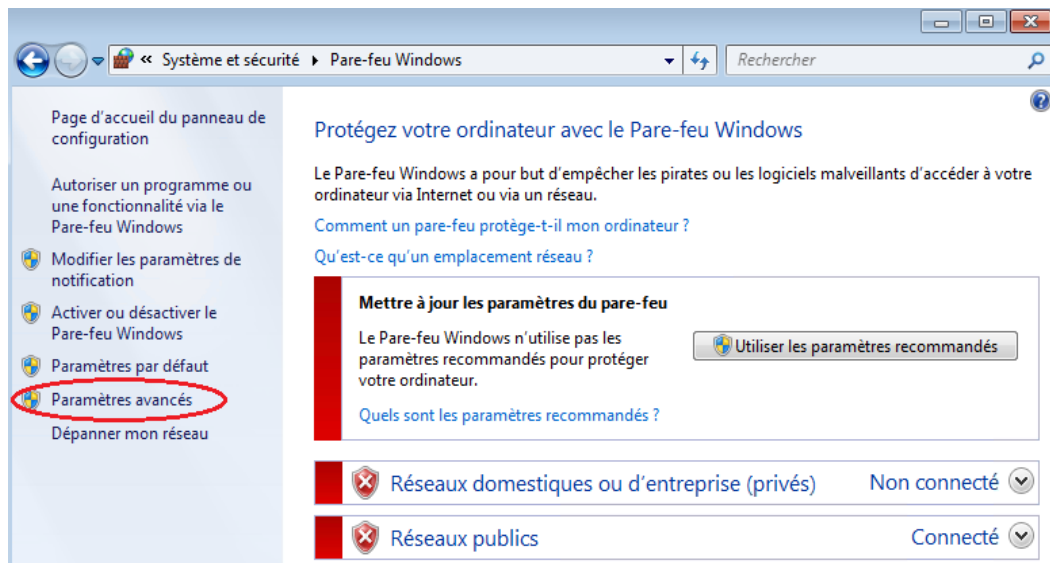
a. À partir du Panneau de configuration, cliquez sur l'option **Système et sécurité**.



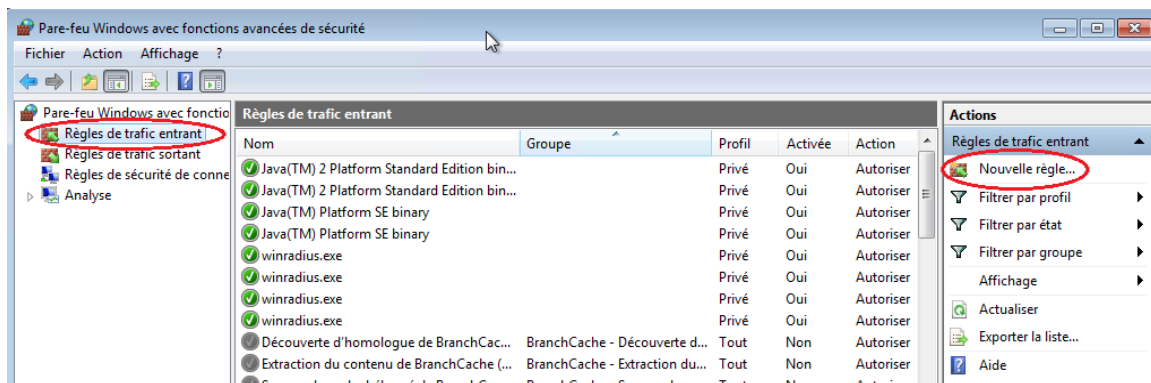
b. Dans la fenêtre Système et sécurité, cliquez sur **Pare-feu Windows**.



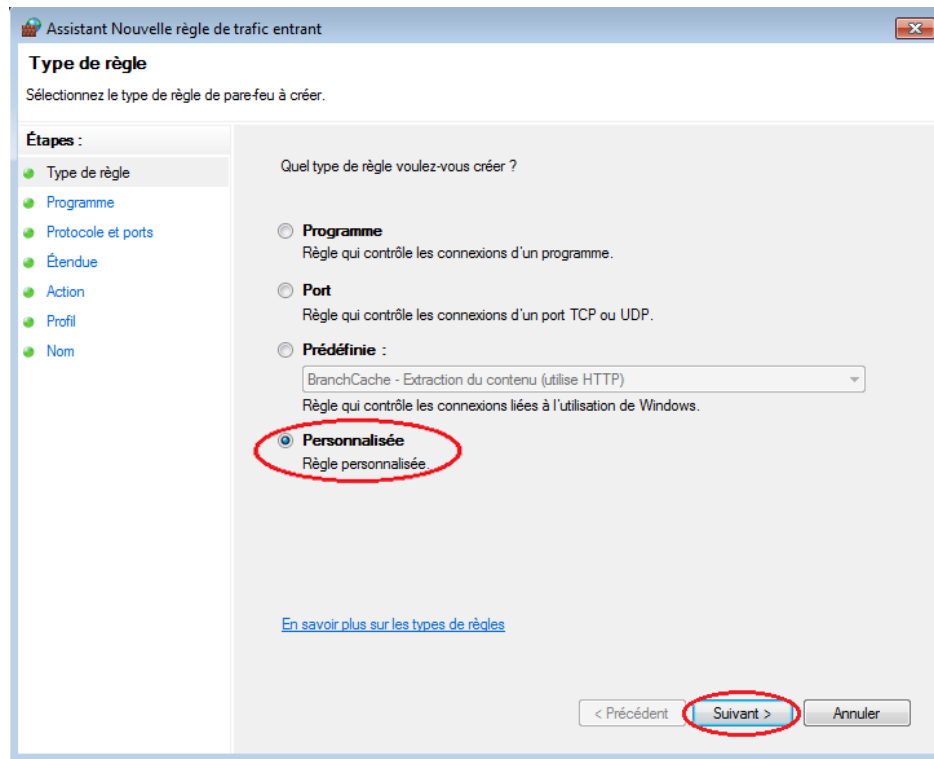
- c. Dans le volet gauche de la fenêtre Pare-feu Windows, cliquez sur **Paramètres avancés**.



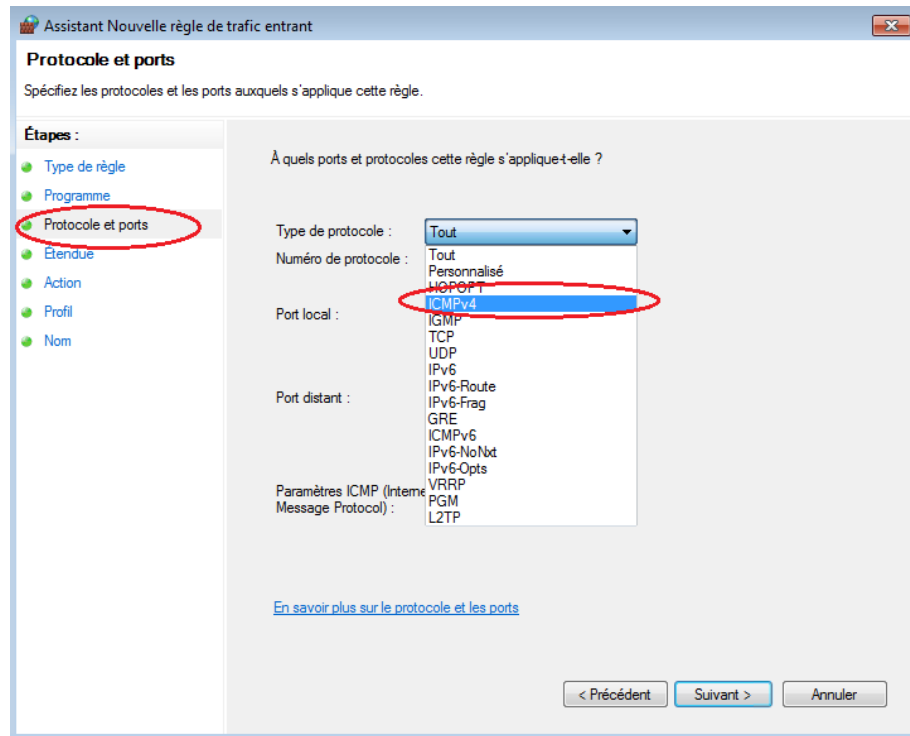
- d. Dans la fenêtre de sécurité avancée, choisissez l'option **Règles de trafic entrant** dans la barre latérale gauche puis cliquez sur **Nouvelle règle...** dans la barre latérale droite.



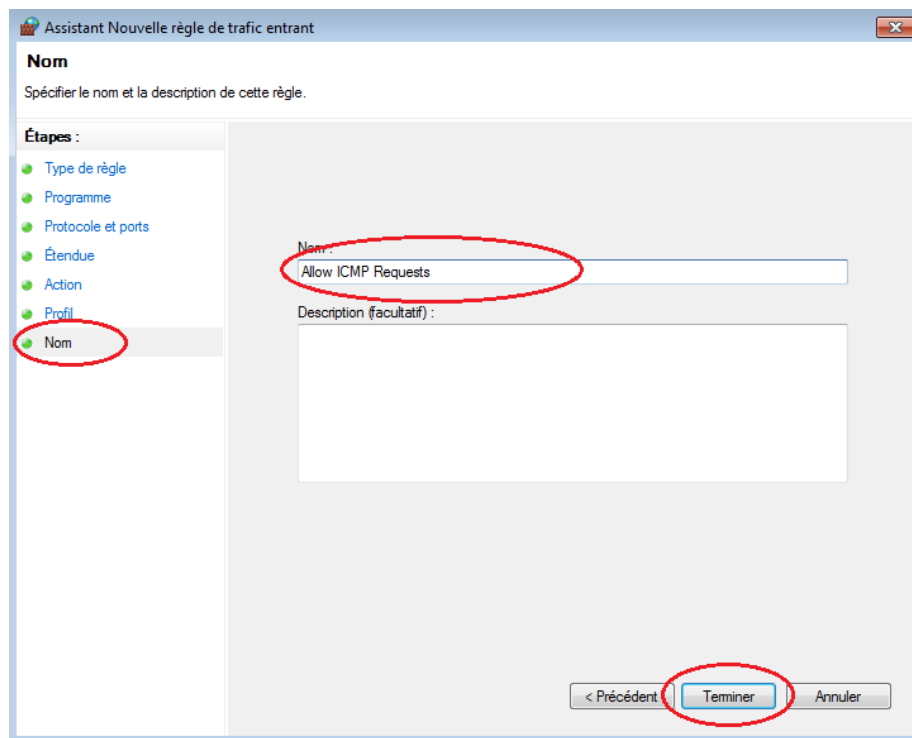
- e. Cette action démarre l'Assistant Nouvelle règle de trafic entrant. Dans l'écran Type de règle, cliquez sur la case d'option Personnalisée, puis cliquez sur **Suivant**.



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



- g. Dans le volet de gauche, cliquez sur l'option **Nom** et dans le champ Nom, tapez **Allow ICMP Requests (Autoriser les requêtes ICMP)**. Cliquez sur **Finish (Terminer)**.

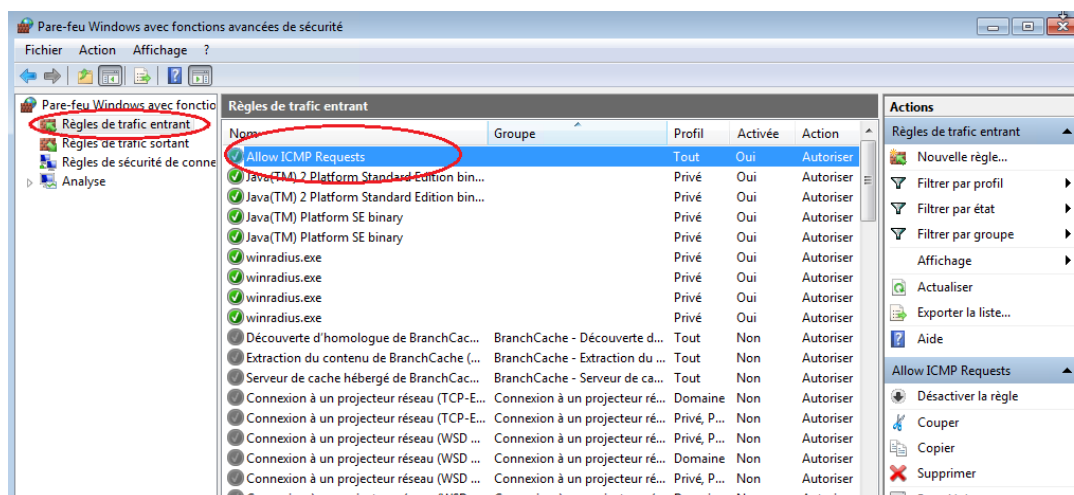


Cette nouvelle règle doit permettre aux membres de votre équipe de recevoir des réponses ping de votre ordinateur.

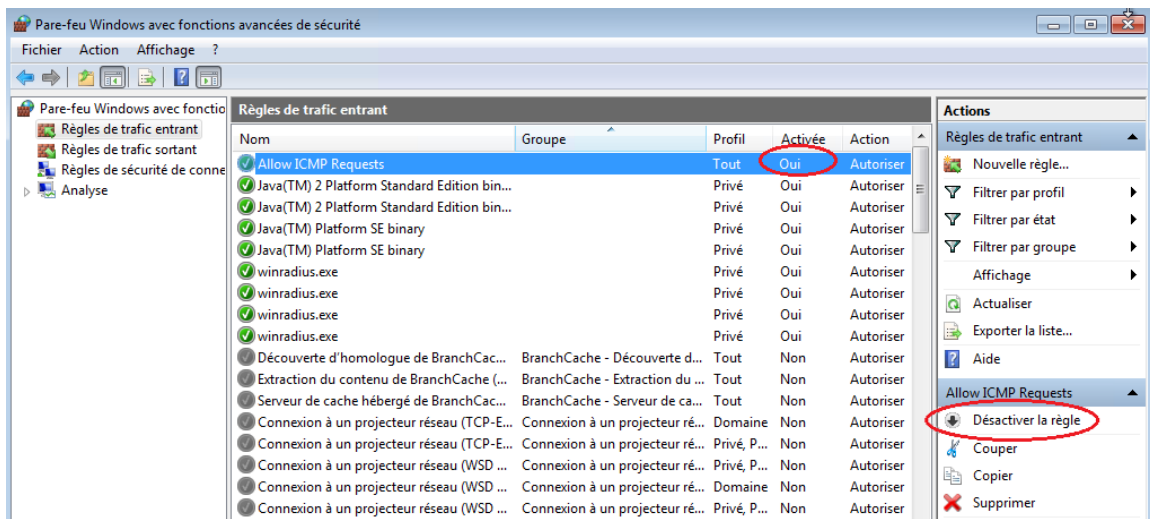
Étape 2 : Désactivation ou suppression de la nouvelle règle ICMP.

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 supprime cette dernière définitivement de la liste des règles de trafic entrant.

- a. Dans la fenêtre de sécurité avancée, dans le volet de 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 apparaît 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.

