TP7: utilisation de Wireshark™ pour afficher des unités de données de protocole

Objectifs pédagogiques

- Expliquer l'objectif d'un analyseur de protocoles (Wireshark)
- Exécuter une capture de base des unités de données de protocole (PDU) à l'aide de Wireshark
- Exécuter une analyse de base des PDU sur un trafic de données réseau simple
- Se familiariser aux fonctionnalités et options de Wireshark telles que la capture des PDU et le filtrage de l'affichage

Contexte

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. Avant juin 2006, Wireshark répondait au nom d'Ethereal.

Un analyseur de paquets (ou analyseur de réseaux ou de protocoles) est un logiciel permettant d'intercepter et de consigner le trafic des données transférées sur un réseau de données. L'analyseur « capture » chaque 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 programmé pour reconnaître la structure de différents protocoles réseau. Vous pouvez l'utiliser pour afficher l'encapsulation et les champs spécifiques aux PDU, puis interpréter leur signification.

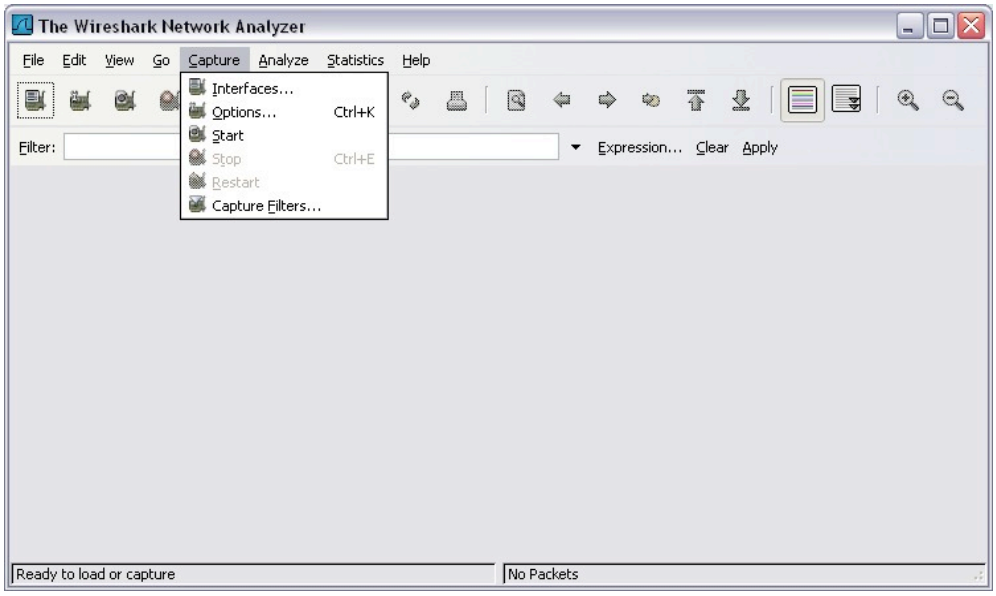
Cet outil est utile pour toutes les personnes intervenant au niveau des réseaux. Vous pouvez vous en servir dans le cadre de la plupart des travaux pratiques des cours CCNA, à des fins d'analyse de données et de dépannage.

Pour en savoir plus sur cet analyseur et télécharger le programme correspondant, accédez au site http://www.Wireshark.org

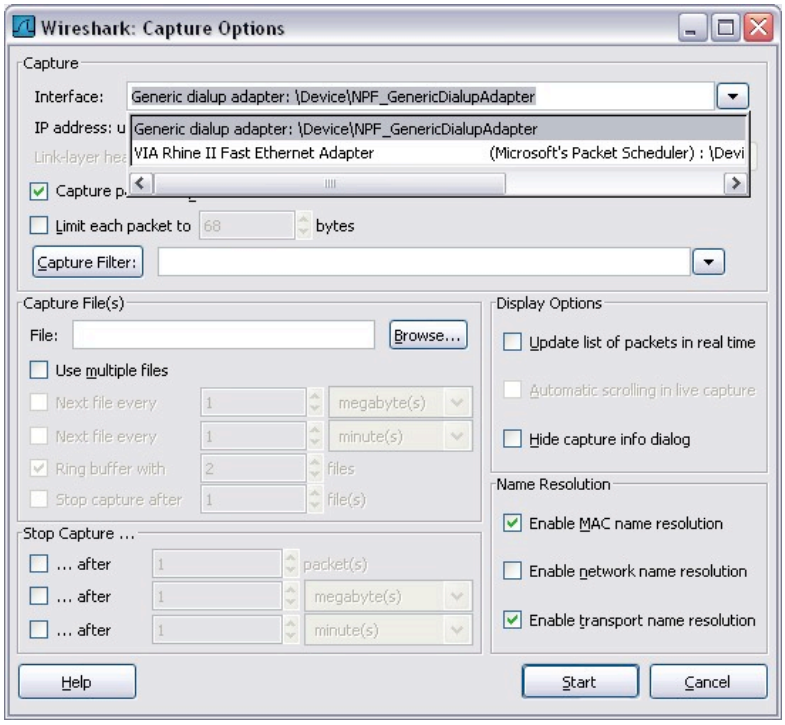
Scénario

Pour pouvoir capturer des données, vous devez d'abord vous connecter au réseau depuis l'ordinateur sur lequel Wireshark est installé et exécuter Wireshark.

Lorsque vous lancez Wireshark, l'écran ci-dessous s'affiche.

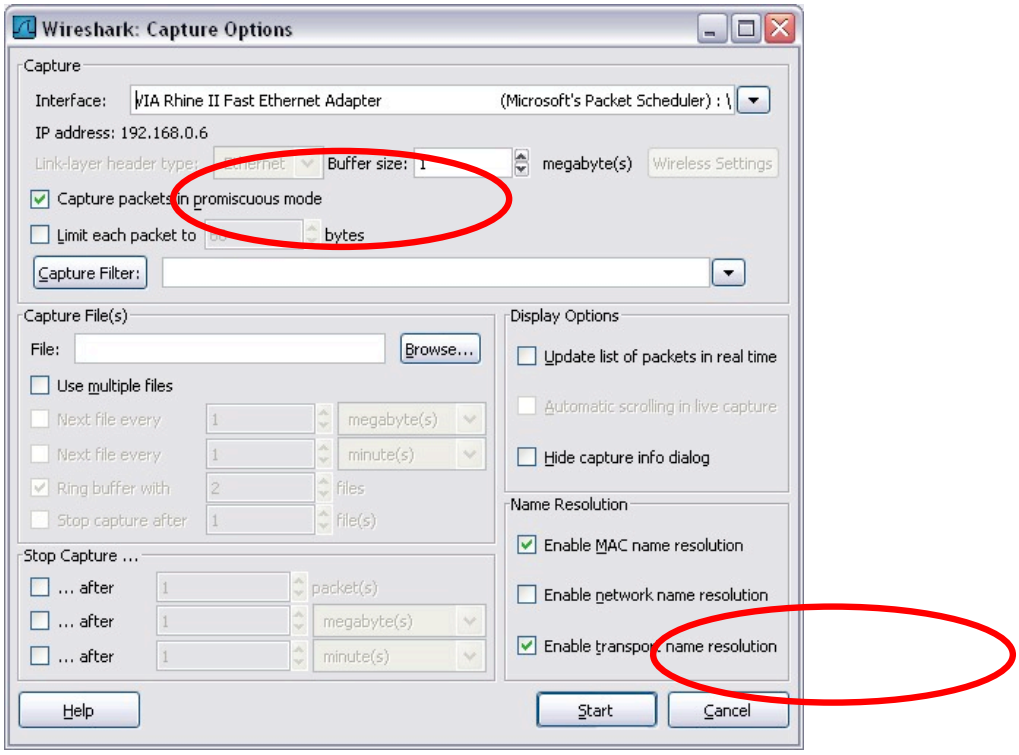


Pour lancer la capture des données, sélectionnez d'abord l'élément **Options** dans le menu **Capture**.
La boîte de dialogue **Options** comprend tout un ensemble de paramètres et de filtres déterminant le trafic de données capturé et le mode de capture utilisé.



Vous devez commencer par vous assurer que Wireshark est configuré pour l'interface appropriée. Dans la liste déroulante **Interface**, sélectionnez la carte réseau utilisée. Pour un ordinateur, il s'agit généralement de la carte Ethernet connectée.

Vous pouvez ensuite définir les **Capture options**. Examinez les deux options mises en relief ci-dessous.



Configuration de Wireshark permettant de capturer des paquets en mode de proximité

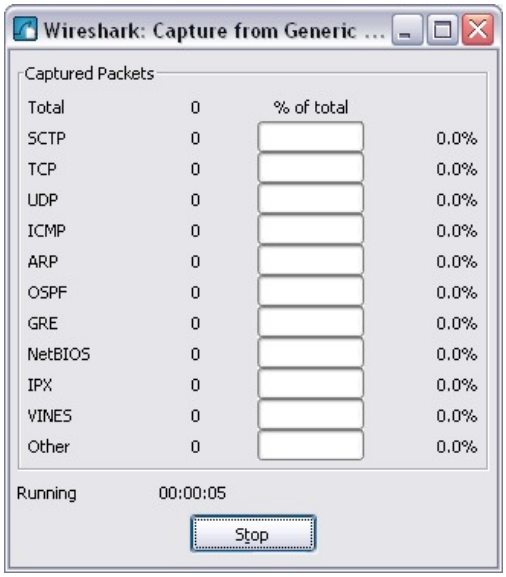
Si vous ne sélectionnez pas l'option Capture packets in promiscious mode, seules les PDU destinées à l'ordinateur sont capturées.
Si vous la sélectionnez, toutes les PDU destinées à l'ordinateur et toutes celles détectées par la carte réseau de l'ordinateur sur le même segment de réseau (c'est-à-dire les PDU transitant par la carte réseau non destinées à l'ordinateur) sont capturées.
Remarque : la capture de ces PDU supplémentaires dépend du périphérique utilisé pour connecter les ordinateurs finaux sur le réseau. Les résultats d'analyse Wireshark varient en fonction des différents périphériques (concentrateurs, commutateurs, routeurs) utilisés au cours de la formation.

Configuration de Wireshark permettant de résoudre les noms réseau

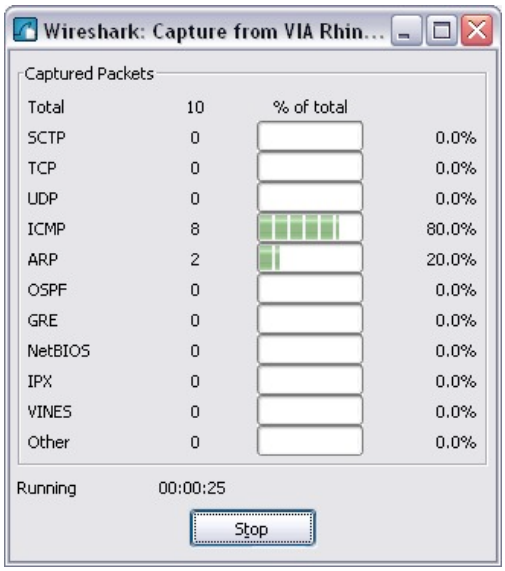
Utilisez l'option Enable... name resolution pour indiquer si Wireshark doit convertir les adresses réseau détectées dans les PDU en noms. Bien que cette fonction soit utile, notez que le processus de résolution des noms risque d'ajouter des PDU aux données capturées et ainsi peut-être de fausser l'analyse.

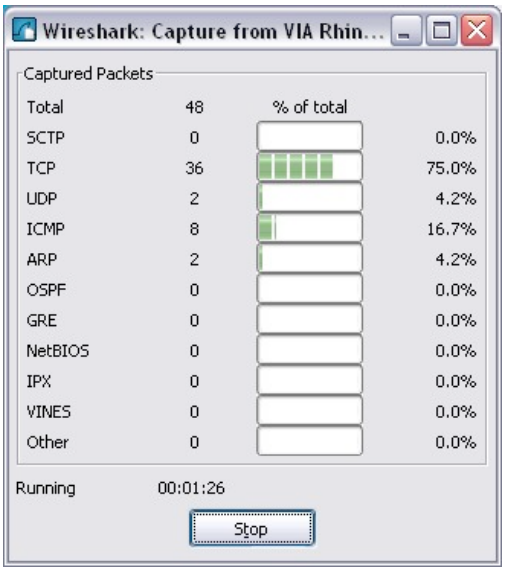
Un certain nombre d'autres paramètres de filtrage et processus de capture sont également disponibles.

Cliquez sur le bouton **Start** (Démarrer) pour lancer la capture des données. Une fenêtre affiche l'état d'avancement.



Le type et le nombre de PDU capturées sont indiqués au fur et à mesure du déroulement du processus.

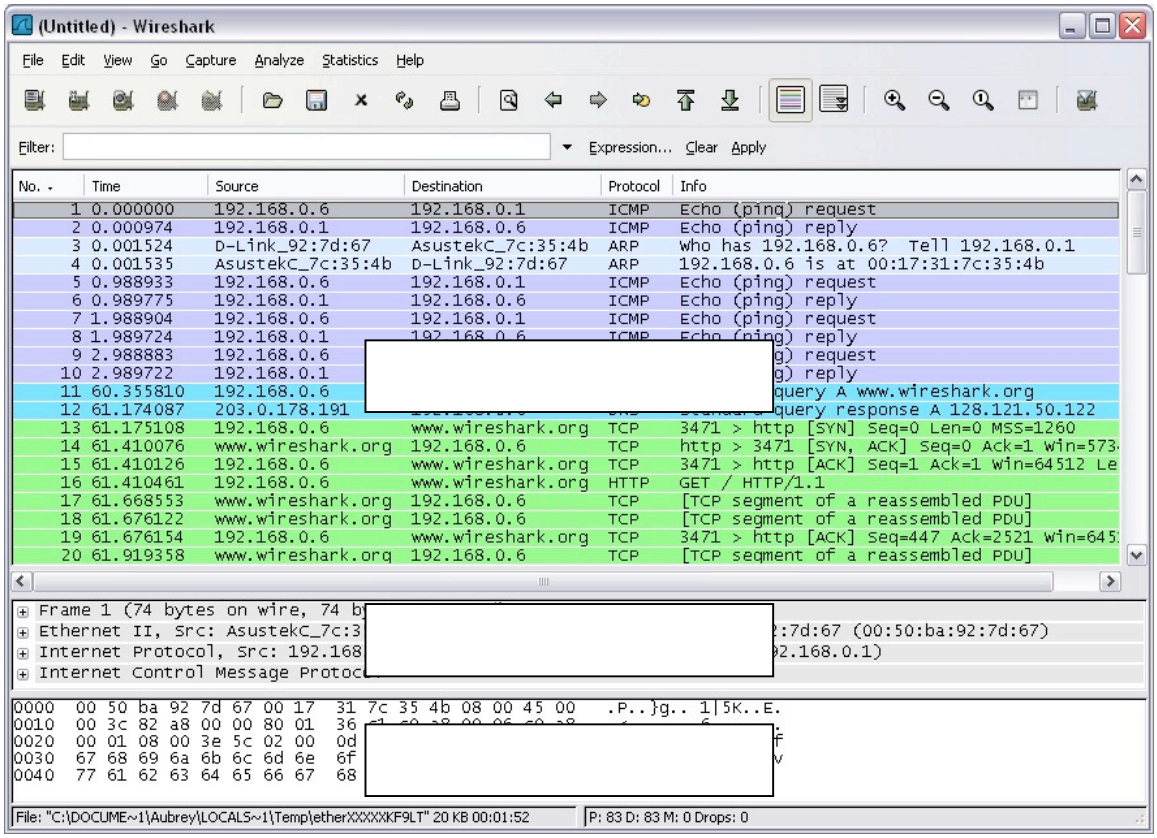




Les exemples ci-dessus montrent la capture d'un processus ping suivi d'un accès à une page Web.

Cliquez sur le bouton **Stop** pour mettre fin à la capture. L'écran principal s'affiche.

La fenêtre principale de Wireshark est constituée de trois volets.



Le volet supérieur de l'écran présenté ci-dessus comprend un récapitulatif des PDU (ou paquets) capturées. Le contenu des deux autres volets dépend des paquets sélectionnés au sein de ce volet.

Le volet du milieu comprend des informations détaillées sur le paquet sélectionné dans le premier volet.

Enfin, le volet inférieur affiche les données (au format hexadécimal correspondant à la représentation binaire) issues du paquet sélectionné dans le premier volet, en mettant en surbrillance les éléments correspondant au champ sélectionné dans le volet du milieu.

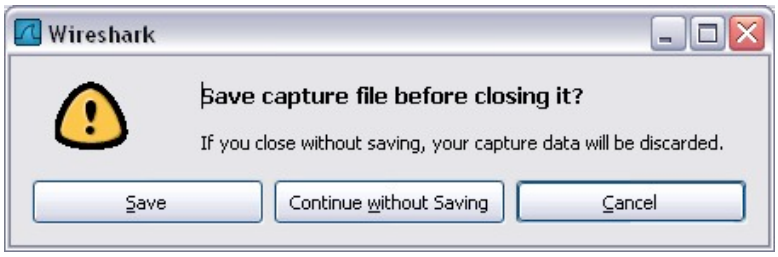
Chaque ligne de la liste des paquets (premier volet) correspond à une PDU (un paquet) de données capturée. Si vous sélectionnez une ligne dans ce volet, ses détails s'affichent dans les volets du milieu et inférieur. Dans l'exemple ci-dessus, le volet supérieur comprend les PDU capturées lors de l'utilisation d'une commande ping et d'un accès au site http://www.Wireshark.org. Le paquet numéro 1 est sélectionné.

Le volet du milieu affiche les détails de ce paquet. Les protocoles et les champs de protocole du paquet sélectionné sont indiqués. Ils s'affichent sous la forme d'une arborescence que vous pouvez développer ou réduire.

Le volet inférieur présente les données du paquet sélectionné dans le volet supérieur au format « hexdump ». Ce volet ne sera pas examiné en détail au cours de la présente session de travaux pratiques. Notez toutefois que ces informations sont utiles lors des analyses plus approfondies car elles permettent de passer en revue les valeurs binaires et le contenu des PDU.

Vous pouvez enregistrer les informations capturées pour les PDU de données dans un fichier. Le fichier peut ensuite être ouvert dans Wireshark en vue d'une analyse ultérieure sans qu'il soit nécessaire de capturer à nouveau le trafic de données. Les informations qui s'affichent lorsque vous ouvrez un fichier de capture sont identiques à celles de la capture d'origine.

Vous êtes invité à enregistrer les PDU capturées lorsque vous fermez un écran de capture ou que vous quittez Wireshark.



Cliquez sur **Continue without Saving** (Poursuivre sans enregistrer) pour fermer le fichier ou quitter Wireshark sans enregistrer les données capturées.

Tâche 1 : capture des PDU associées à un processus ping

Étape 1 : vérification de la topologie et de la configuration standard utilisées dans le cadre des travaux pratiques et lancement de Wireshark sur un ordinateur de pod

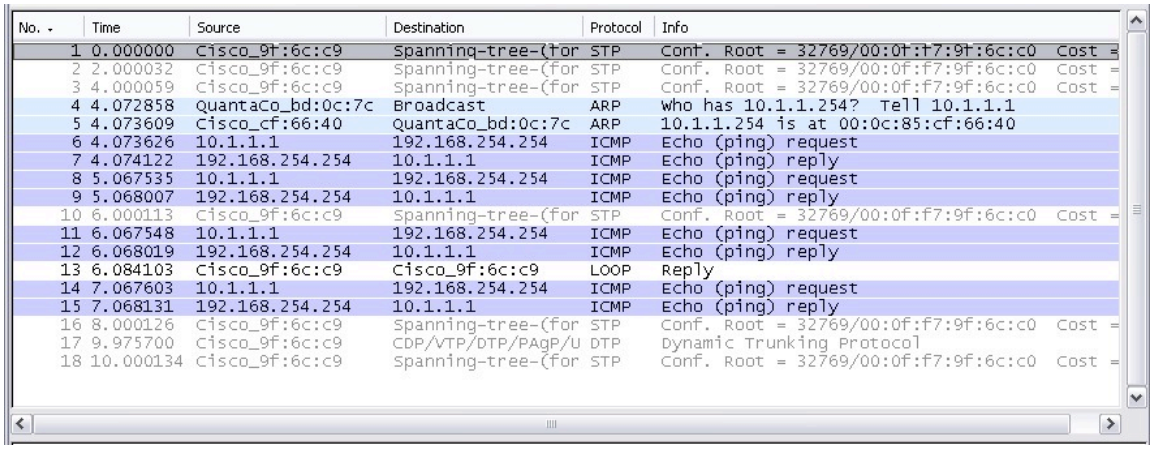
Définissez les options de capture comme indiqué ci-dessus, dans la présentation, puis lancez la capture.

Sur la ligne de commande de l'ordinateur, envoyez une commande ping à l'adresse IP ///d'un autre périphérique connecté au réseau (voir le schéma de la topologie fourni pour cette session de travaux pratiques). Ici, il s'agit d'une commande ping envoyée au serveur Eagle en spécifiant l'adresse **192.168.254.254**.

Une fois que vous avez reçu le résultat attendu, arrêtez la capture des paquets.

Étape 2 : observation du volet de la liste des paquets

Le volet supérieur de Wireshark doit ressembler à ce qui suit :



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Examinez les paquets de la liste ci-dessus, notamment les paquets 6, 7, 8, 9, 11, 12, 14 et 15.

Localisez les paquets équivalents au sein de la liste de paquets affichée sur votre ordinateur.
Si vous avez effectué l'étape 1A ci-dessus, faites le lien entre les messages affichés dans la fenêtre de ligne de commande suite à l'envoi de la commande ping et les six paquets capturés par Wireshark.

Observez la liste des paquets de Wireshark et répondez aux questions suivantes :

Quel protocole est utilisé avec la commande ping ? _____

Quel est le nom complet du protocole ? _____

Quels sont les noms des deux messages ping ? _____

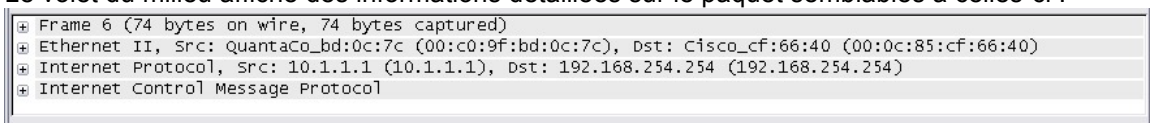
_____

Vous attendiez-vous à obtenir les adresses IP source et de destination indiquées ? Oui/Non

Pourquoi ? _____

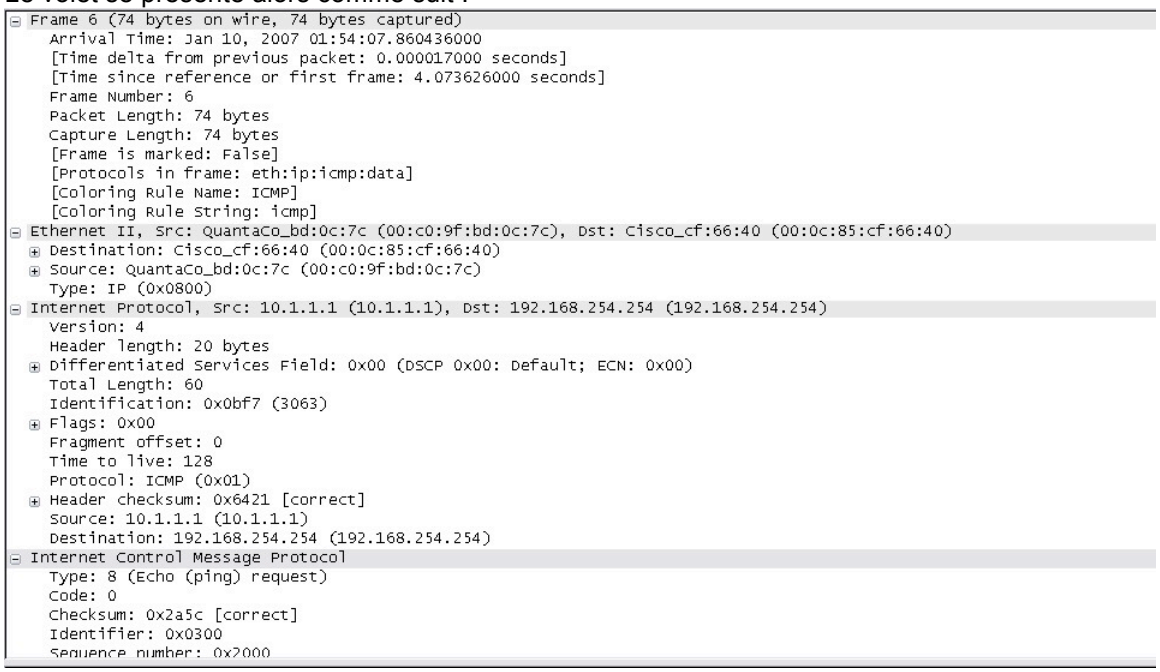
Étape 3 : sélection (mise en surbrillance) du premier paquet de requête d'écho de la liste à l'aide de la souris

Le volet du milieu affiche des informations détaillées sur le paquet semblables à celles-ci :



Cliquez sur les quatre signes « **+** » pour développer les arborescences correspondantes.

Le volet se présente alors comme suit :



Comme vous pouvez le constater, vous pouvez développer encore chaque section et protocole. Consacrez un peu de temps à l'étude de ces informations. Il se peut que vous ne compreniez pas toutes les informations affichées à ce stade du cours, mais notez toutefois celles que vous reconnaissez.

Localisez les deux types de « Source » et « Destination » différents. Pourquoi y en a-t-il deux ?

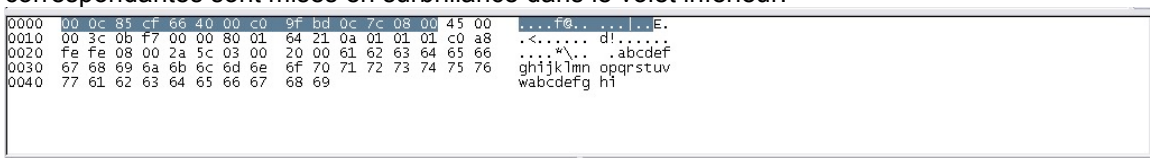
_____

Quels sont les protocoles inclus dans la trame Ethernet ?

_____

Lorsque vous sélectionnez une ligne dans ce volet, tout ou partie des informations correspondantes sont mises en surbrillance dans le volet inférieur des octets associés aux paquets.

Par exemple, si vous sélectionnez la deuxième ligne (+ Ethernet II) dans le volet du milieu, les valeurs correspondantes sont mises en surbrillance dans le volet inférieur.



Il s'agit des valeurs binaires spécifiques à ces informations concernant la PDU. Il n'est pas nécessaire de comprendre toutes ces informations en détail à ce stade du cours.

Étape 4 : sélection de l'élément Close (Fermer) dans le menu File (Fichier)

Lorsque ce message s'affiche, cliquez sur **Continue without Saving** (Poursuivre sans enregistrer).

Tâche 2 : capture des PDU associées à un processus FTP

Étape 1 : lancement de la capture des paquets

En supposant que Wireshark soit toujours en cours d'exécution suite aux étapes précédentes, cliquez sur l'option **Start** (Démarrer) du menu **Capture** de Wireshark pour lancer la capture des paquets.

Tapez **ftp 192.168.254.254** au niveau de la ligne de commande de l'ordinateur sur lequel Wireshark est exécuté.

Une fois la connexion établie, spécifiez l' ID utilisateur **anonymous** sans mot de passe.
Userid: **anonymous**
Password: <ENTRÉE>
Vous pouvez également utiliser l'ID utilisateur **cisco** et le mot de passe **cisco**.

Une fois connecté, tapez **`get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe`**, puis appuyez sur la touche <ENTRÉE>. Le processus de téléchargement du fichier à partir du serveur ftp démarre. Vous obtenez un résultat semblable à celui-ci :

```
C:\Documents and Settings\ccna1>ftp eagle-server.example.com
Connected to eagle-server.example.com.
 220 Welcome to the eagle-server FTP service.
User (eagle-server.example.com:(none)): anonymous
331 Please specify the password.
Password:<ENTRÉE>
230 Login successful.
ftp> get /pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe
200 PORT command successful. Consider using PASV.
150       Opening       BINARY       mode       data       connection       for
pub/eagle_labs/eagle1/chapter1/gaim-1.5.0.exe (6967072 bytes).
226 File send OK.
ftp: 6967072 bytes received in 0.59Seconds 11729.08Kbytes/sec.
```

Une fois le fichier téléchargé, tapez **quit :**

```
ftp> quit
221 Goodbye.
C:\Documents and Settings\ccna1>
```

Arrêtez ensuite la capture des PDU dans Wireshark.

Étape 2 : agrandissement du volet de la liste des paquets de Wireshark et passage en revue des PDU répertoriées

Localisez et notez les PDU associées au téléchargement du fichier.
Il s'agit des PDU issues du protocole TCP de la couche 4 et du protocole FTP de la couche 7.

Identifiez les trois groupes de PDU associés au transfert du fichier.

Si vous avez effectué l'étape ci-dessus, faites le lien entre les paquets et les messages et invites de la fenêtre de ligne de commande FTP.

Le premier groupe correspond à la phase de connexion au serveur.
Fournissez quelques exemples de messages échangés au cours de cette phase.

_____

Localisez et notez quelques exemples de messages échangés au cours de la deuxième phase, c'est-à-dire celle de la requête de téléchargement et du transfert de données.

_____

_____

Le troisième groupe de PDU se rapporte à la déconnexion.
Fournissez quelques exemples de messages échangés au cours de cette phase.

_____

_____

Localisez les échanges TCP récurrents au cours du processus FTP. Quels types d'opérations TCP indiquent-ils ?

_____

_____

Étape 3 : analyse des informations détaillées sur les paquets

Sélectionnez (mettez en surbrillance) un paquet de la liste associé à la première phase du processus FTP.
Observez ses détails dans le volet du milieu.

Quels sont les protocoles encapsulés dans la trame ?

_____

Sélectionnez les paquets contenant le nom d'utilisateur et le mot de passe.
Examinez la partie mise en surbrillance dans le volet des octets.

Que pouvez-vous en déduire sur la sécurité de ce processus de connexion FTP ?

_____

Sélectionnez un paquet associé à la deuxième phase.
À partir de n'importe quel volet, localisez le paquet comportant le nom du fichier.

Le nom de fichier est : _____

Sélectionnez un paquet comportant le contenu du fichier ; notez le texte brut visible dans le volet des octets.

Dans les volets des informations détaillées et des octets, sélectionnez puis examinez quelques paquets échangés au cours de la troisième phase correspondant au téléchargement du fichier.
Qu'est-ce qui différencie le contenu de ces paquets ?
_____

Une fois terminé, fermez le fichier Wireshark en choisissant l'option Continue without Saving (Poursuivre sans enregistrer).

Tâche 3 : capture des PDU associées à un processus HTTP

Étape 1 : lancement de la capture des paquets

En supposant que Wireshark soit toujours en cours d'exécution suite aux étapes précédentes, cliquez sur l'option **Start** (Démarrer) du menu **Capture** de Wireshark pour lancer la capture des paquets.

Remarque : vous n'avez pas besoin de définir les options de capture si vous effectuez cette étape à la suite des étapes précédentes de cette session de travaux pratiques.

Ouvrez un navigateur Web sur l'ordinateur sur lequel vous exécutez Wireshark.
Saisissez l'URL du serveur Eagle de **example.com** ou bien l'adresse IP 192.168.254.254. Une fois la page Web téléchargée dans son intégralité, arrêtez la capture des paquets dans Wireshark.

Étape 2 : agrandissement du volet de la liste des paquets de Wireshark et passage en revue des PDU répertoriées

Localisez et identifiez les paquets TCP et HTTP associés au téléchargement de la page Web.

Notez les similarités qui existent entre cet échange de messages et celui du processus FTP.

Étape 3 : mise en surbrillance d'un paquet HTTP du volet supérieur portant la mention « (text/html) » au niveau de la colonne Info

Dans le volet des détails de paquet (volet du milieu), cliquez sur le signe « + » situé en regard de **Line-based text data: html"**
Quel type d'informations s'affiche-t-il lorsque vous développez cet élément ?
_____

Examinez la partie mise en surbrillance dans le volet des octets.
Elle indique les données HTML transportées par le paquet.

Une fois terminé, fermez le fichier Wireshark en choisissant l'option Continue without Saving (Poursuivre sans enregistrer).

Tâche 4 : réflexion

Examinez les informations d'encapsulation relatives aux données réseau capturées fournies par Wireshark. Faites-les correspondre aux modèles de couche TCP/IP et OSI. Il est important que vous puissiez reconnaître et associer les deux protocoles représentés et les ///types de couche de protocole et d'encapsulation des modèles aux informations fournies par Wireshark.

Tâche 5 : travaux pratiques avancés

Discutez de l'utilité des analyseurs de protocoles tels que Wireshark dans le cadre des opérations suivantes :

(1) Résolution d'un problème de téléchargement de page Web sur le navigateur d'un ordinateur

et

(2) Identification du trafic des données demandées par les utilisateurs sur un réseau

_____

_____

_____

_____

_____

_____

_____

Tâche 6 : nettoyage

Sauf indication contraire de la part du formateur, quittez Wireshark et arrêtez votre ordinateur de façon appropriée.