

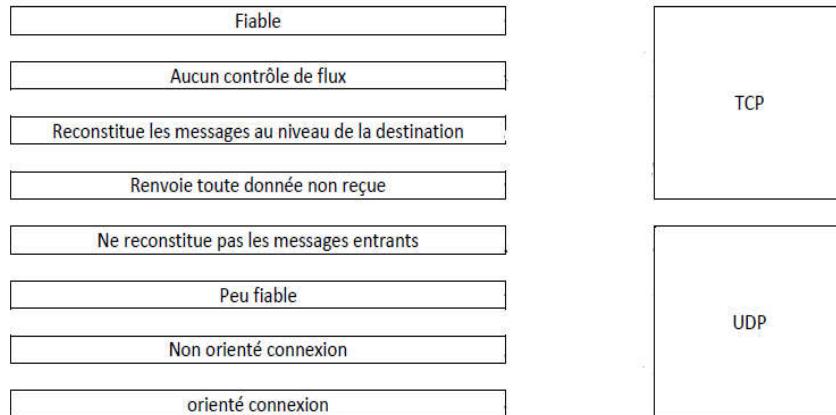
TP N°2

Objectifs

- Comprendre le modèle Tcp/IP:
- Découvrir les caractéristiques générales et l'encapsulation des protocoles du modèle "TCP/IP"
- Être capable d'utiliser un analyseur de protocoles.

Partie exercices

1. Comment les protocoles TCP et IP sont-ils identifiés dans une trame Ethernet ?
2. Quels sont les avantages d'UDP sur TCP ??
3. A quoi correspondent les numéros de port ? Quels paramètres TCP/IP sont nécessaires pour établir une connexion TCP ?
4. On suppose qu'une connexion TCP est ouverte entre deux utilisateurs A et B. Comment sont traités les segments dans les deux cas suivants :
 - L'émetteur et le récepteur sont connectés au même réseau de type TCP/IP ?
 - L'émetteur et le récepteur appartiennent à deux réseaux distincts utilisant TCP/IP, interconnectés grâce à un routeur IP ?
5. Classez les propositions en fonctions du protocole qu'elles décrivent (TCP ou UDP).



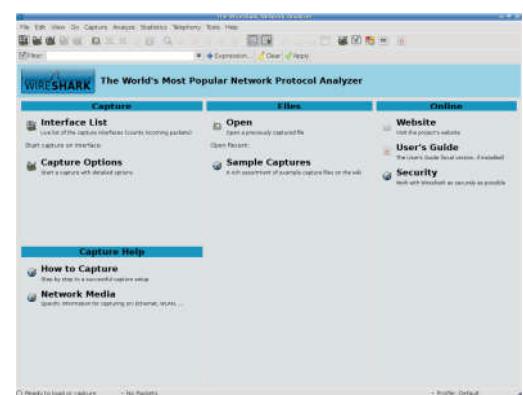
6. Dans la couche transport, lequel des contrôles suivants permet d'éviter qu'un hôte transmette des données provoquant un dépassement de capacité des mémoires tampons de l'hôte en réception ?
 - a. Le niveau de service Best effort
 - b. Le chiffrement
 - c. Le contrôle de flux
 - d. Le contrôle de congestion
 - e. La prévention d'encombrement

7. Lors du transfert des données, quelles sont les principales responsabilités de l'hôte récepteur ?
 - a. Le débit
 - b. L'encapsulation
 - c. L'accusé de réception
 - d. La bande passante
 - e. La segmentation
 - f. Le réassemblage
8. Qu'est-ce qui détermine la quantité de données que peut transmettre une station émettrice exécutant le protocole TCP/IP avant qu'elle doive recevoir un accusé de réception ?
 - a. La taille du segment
 - b. Le débit de transmission
 - c. La bande passante
 - d. La taille de fenêtre
 - e. Le numéro de séquence
9. Quelle est la fonction du numéro d'ordre inclus dans l'en-tête TCP/IP ?
 - a. Il réassemble les segments en données complètes
 - b. Il identifie le protocole de la couche application
 - c. Il indique le numéro de l'octet suivant attendu
 - d. Il précise le nombre maximal d'octets autorisés lors d'une session
10. Quelle est le fonction du numéro de ports TCP/UDP ?
 - a. Ils permettent d'indiquer le début d'un échange en trois étapes
 - b. Ils permettent de réorganiser les segments dans l'ordre adéquat
 - c. Ils permettent d'identifier le nombre de paquets de données pouvant être envoyés sans accusé de réception
 - d. Ils permettent de suivre les différentes conversations simultanées dans un réseau
11. Citez trois techniques qui rendent TCP fiables ;
12. Décodez le segment TCP ci-après, donné en hexadécimal :
00 15 0F 87 9C CB 7E 01 27 E3 EA 01 50 12 10 00 DF 3D 00 00

Partie pratique

Présentation de wireshark

Wireshark (anciennement Ethereal) est un logiciel libre analyseur de protocole réseau. Il permet de visualiser et de capturer les trames, les paquets de différents protocoles réseau, filaire ou pas, il s'appelle aussi « packet sniffer », utilisé dans le dépannage et l'analyse de réseaux informatiques. Wireshark est multiplateformes. Site officiel <http://www.wireshark.org/>, Vérifier si le logiciel Wireshark est installé sur votre poste.



Le logiciel s'ouvre sur cette page de menu :

Nous utilisons essentiellement le menu « Open » qui permettra de charger un fichier de capture pour analyser. Ouvrez le fichier http.cap disponible sur le serveur ou sur le site <http://wiki.wireshark.org/SampleCaptures>.

L'affichage se décompose en trois cercles

Cercle (1) : Filtrage

Il est possible de créer des filtres d'affichage sur liste l'ensemble des paquets capturés, qui ne montrent que les trames conformes à la règle de filtrage. Cela permettra d'isoler un échange en particulier ou l'analyse d'un protocole spécifique.

Le bouton « Expression » permet d'accéder à un assistant pour créer une règle de filtrage. Une règle de filtrage s'appuie sur les champs des entêtes (header) des protocoles connus du logiciel Wireshark

Cercle (2) : Encapsulation

Le cercle 2 affiche le détail d'un paquet sélectionné ce qui illustre le principe de l'encapsulation des protocoles utilisées dans l'échange d'une trame. On fait souvent référence à un modèle pour représenter cette communication. Ici, le modèle est celui qui implémente les protocoles de la famille « TCP/IP »

Par exemple :

En sachant qu'une couche se décomposera en deux parties comprenant un entête

(header) appelé aussi PCI (Protocol Control Information) et un champ DATA (au sens « network data »). En fait, cela représente les protocoles présents dans la trame de la manière suivante :

trame



On comprend alors que le champ DATA d'une couche contient le bloc de la couche supérieure (Header + DATA). C'est le principe de l'encapsulation.

Cercle (3) : Détail en hexadécimal

présente l'ensemble du paquet sous forme octale et ASCII. Ces octets contiennent les en-têtes des différentes couches de l'architecture TCP/IP ainsi que les données transmises par le processus à l'origine du message.

Travail à réaliser

1- Lecture d'une trace

1. Télécharger la trace (la capture) de l'adresse (<http://packetlife.net/captures/HTTP.cap>)

2. Ouvrir Wireshark, Aller dans File->Open puis choisir le fichier téléchargé en 1.

3. Examiner le fichier ouvert et répondre aux questions suivantes

Questions :

1. Enumérer les colonnes du tableau du centre, quels est le sens de chacune ?

2. Positionner le curseur sur la ligne N°1 et examiner le contenu du tableau en dessous.

Enumérer la liste des protocole que vous reconnaissiez. Quel est le numéro du protocole IP dans une trame Ethernet ?

3. Dans un tableau approprié indiquer pour les trois premières frames (1,2,3), les valeurs des champs suivants : Champs @IP-Source @IP-Destination, Port-Source, Port-Destination,

Flags, champs numéro de séquence, champs numéro acquittement. Quelle l'est l'adresse IP du client dans ce dialogue ? Et celle du serveur ? Comment avez-vous fait pour les identifier ?

Quels sont les programmes qui sont en communication C/S ? Comment sont-ils identifiés ?

4. La ligne 4 concerne quel protocole de niveau application ? Quel type de message est envoyé ?

Quelle version du protocole de niveau application est utilisée ? Combien d'octets contient-elle ?

5. Continuez à donner les valeurs des champs numéro séquence, numéro acquittement et flagpour le restant des segments. Quelles sont les règles de leur évolution ?

6. Analyser et discuter de la ligne 36. Quelle est la taille de l'image ? Combien de segments TCP a nécessité son envoi ?

7. A quoi est dû la ligne 37 ?

8. Comme pour la question 1, refaites le tableau pour les lignes 38-40. Que pouvez-vous en dire ?

9. Faites un graphe montrant l'évolution de la fenêtre d'émission du serveur vers le client. Discutez-là.

10. Re-examiner maintenant le champs Options TCP des trois premières lignes . Les lignes à partir de 4 les contient-elles toutes ? Qu'en concluez-vous ? Quelle(s) RFC(s) décrit chaque option ? Pour chaque option indiquer son utilité (contrôle de congestion, contrôle de flux, connexion fiable,etc...).

The first screenshot shows the 'Capture list' window with several frames listed. Frame 1 is highlighted with a red circle and labeled 'Cadré 1 : trames capturées (capture en temps réel possible)'. The second screenshot shows the 'Selected frame details' window for frame 1, also with a red circle around it and labeled 'Cadré 2 : contenu décodé (cadré par cadré) de la trame sélectionnée dans le cadre 1'. The third screenshot shows the 'Hex dump' window for frame 1, with a red circle around it and labeled 'Cadré 3 : "dump" en hexadécimal du paquet sélectionné dans le cadre 2'.

