École Polytechnique de Montréal
Département Génie Informatique et Génie Logiciel
INF3405 – Réseaux Informatiques

Travail pratique N° 3

Analyse d'applications client-serveur avec WireShark

1. Informations générales

Session	Hiver 2020
Public cible	Étudiants de 1er cycle du cours INF3405
Taille de l'équipe	2 étudiants
Date et lieu de réalisation	À partir du 23 mars 2020 à la maison
Date de remise	Le 15 avril 2020 avant 23h55
Pondération	8 %
Directives particulières	1. Tout rapport sera pénalisé de 5 points s'il est soumis par une équipe dont la taille est différente de deux (02 étudiants), sans l'approbation préalable du chargé de laboratoire. **2. Vous devez impérativement fournir des captures d'écran à chaque question du présent laboratoire. Toute réponse non justifiée sera pénalisée.** **3. Soumission du rapport (en format PDF) par moodle uniquement (http://moodle.polymtl.ca).** **4. Tout retard de soumission du rapport du laboratoire sera pénalisé de 3 points par heure de retard.**
Chargé de laboratoire	Bilal Itani (bilal.itani@polymtl.ca) - Gr.01 Liliane-Caroline Demers (liliane-caroline-2.demers@polymtl.ca) - Gr.02 Esther Guerrier (esther.guerrier@polymtl.ca) - Gr.03
Version originale :	Bilal Itani, Mehdi Kadi

2. Connaissances préalables

- Pile de protocole TCP/IP
- Encapsulation des données

- Format des trames Ethernet (802.3)

3. Environnement et outils nécessaires

- Analyseur de protocoles **Wireshark**
- Editeur de fichier **WinHex**

4. Éléments de contexte

Les réseaux d'aujourd'hui présentent des architectures de plus en plus complexes au regard des protocoles impliqués dans leur fonctionnement. La localisation et la résolution de certains dysfonctionnements sont inhérentes à la tâche d'administration d'un réseau. L'analyseur de protocoles demeure l'un des outils les plus importants pour situer de manière précise certains dysfonctionnements identifiés.

Lors de son utilisation, l'analyseur de protocole place l'interface réseau dans un mode appelé *promiscuous* ou banalisé. Dans ce mode de fonctionnement, toute trame reçue sur la carte réseau est remontée à l'analyseur de protocoles et affichée à l'intérieur de celui-ci. Ce mode de fonctionnement diffère du fonctionnement normal, où la carte réseau rejette systématiquement toute trame qui n'est pas destinée au poste hôte (Adresse MAC et IP différents de ceux de l'interface réseau).

Durant votre carrière, vous serez certainement appelés à effectuer du déverminage sur les différentes applications que vous développerez. Pour des applications réseau, il peut être possible que le réseau fasse défaut. Plutôt que de perdre un temps fou à déverminer votre application, il peut être judicieux d'utiliser un analyseur de protocole afin d'identifier si le problème ne se trouve pas au niveau du réseau tout simplement.

Dans le laboratoire #2, vous avez été introduit à un analyseur de protocole, Omnipeek. Bien que cet outil soit utile pour l'analyse du réseau, il nécessite une licence payante. Le présent laboratoire vous introduit à Wireshark, un autre analyseur de protocole similaire à Omnipeek, mais gratuit.

Dans le laboratoire #1, vous avez conçu une application client-serveur permettant l'application du filtre de Sobel sur des images. Le présent laboratoire consiste d'une part à analyser votre application client-serveur du laboratoire 1 et d'autre part à analyse une application "secrète" où vous serez amenés à découvrir ce qu'elle fait en analysant le réseau.

5. Objectifs du laboratoire

- Se familiariser avec Wireshark;
- Comprendre les divers types de paquets qui circulent dans un réseau;
- Visualiser l'encapsulation des données;
- Analyser les échanges réseaux.

Ce travail pratique consiste, par la même occasion, à évaluer quatre des 12 qualités de l'ingénieur définies par le BCAPG (Bureau canadien d'agrément des programmes de génie). Le Bureau d'agrément a pour mandat d'attester que les futurs ingénieurs ont atteint ces 12 qualités à un niveau acceptable. Les quatre qualités en question sont:

Qualité 2 (Analyse de problèmes) : capacité d'utiliser les connaissances et les principes appropriés pour identifier, formuler, analyser et résoudre des problèmes d'ingénierie complexes et en arriver à des conclusions étayées.

Qualité 3 (Investigation) : capacité d'étudier des problèmes complexes au moyen de méthodes mettant en jeu la réalisation d'expériences, l'analyse et l'interprétation des données et la synthèse de l'information afin de formuler des conclusions valides.

Qualité 5 (Utilisation d'outils d'ingénierie) : capacité de créer et de sélectionner des techniques, des ressources et des outils d'ingénierie modernes et de les appliquer, de les adapter et de les étendre à un éventail d'activités simples ou complexes, tout en comprenant les contraintes connexes.

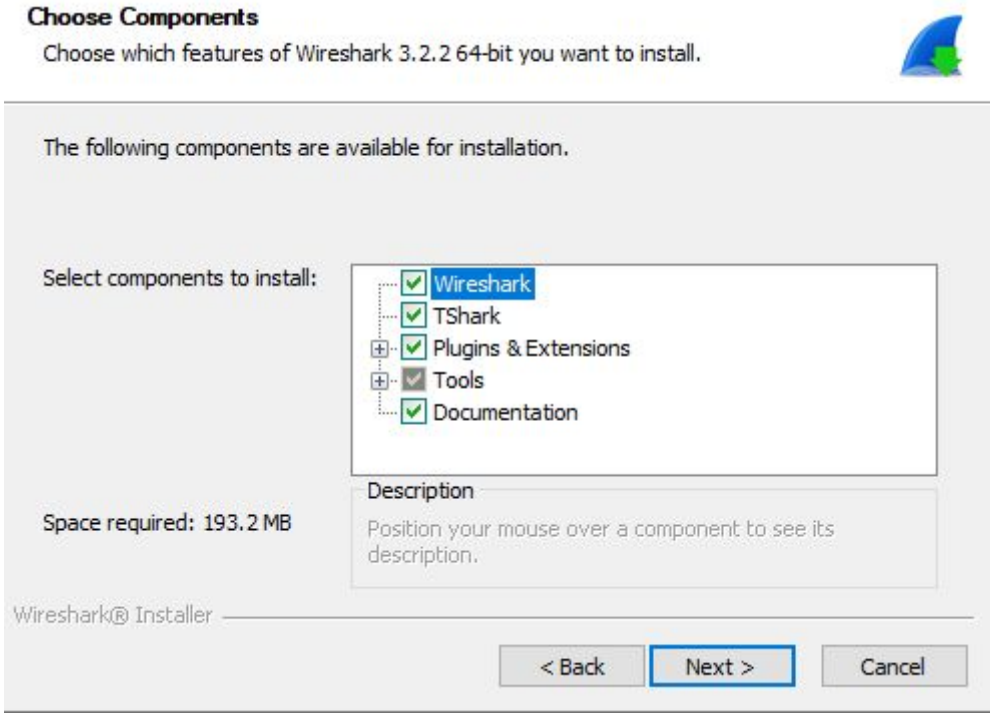
Qualité 9 (Impact du génie sur la société et l'environnement) : capacité à analyser les aspects sociaux et environnementaux de activités liées au génie, notamment comprendre les interactions du génie avec les aspects économiques et sociaux, la santé, la sécurité, les lois et la culture de la société; les incertitudes liées à la prévision de telles interactions; et les concepts de développement durable et de bonne gérance de l'environnement.

6. Préparation de l'environnement de travail client / serveur virtuel

A) Installation de l'outil WireShark sur votre poste de travail

L'outil WireShark est un outil gratuit et open source permettant l'analyse du trafic réseau

1. Télécharger et installer la dernière version stable sur votre poste de travail : https://www.wireshark.org/download.html
2. Pour ce qui est des composantes d'installation, laisser celles par défaut



3. Appuyez sur suivant et garder toutes les options par défaut qu'à la fin de l'installation, il en est de même pour la librairie **Npcap**

B) Installation de l'outil WinHex sur votre poste de travail

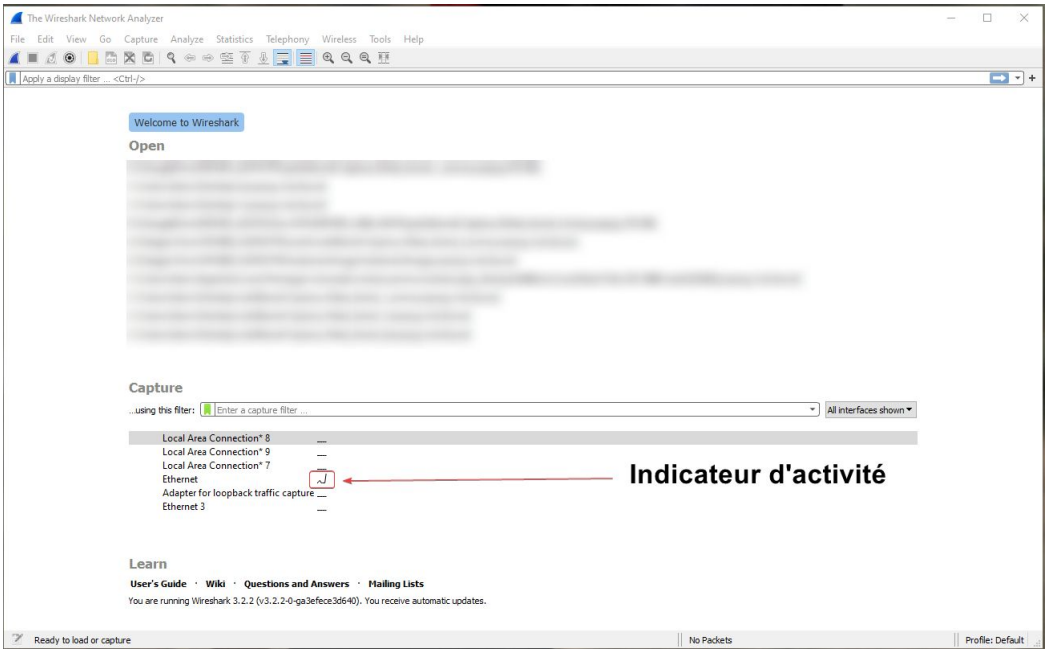
Téléchargez le gratuiciel WinHex, il vous sera utile pour répondre à la question no.7 du laboratoire: http://www.x-ways.net/winhex.zip

Wireshark associe les paquets à des protocoles particuliers dépendamment du port utilisé. Si une application client/serveur utilise le port 5000 pour communiquer, Wireshark déterminera que la communication s'effectue avec le protocole GSM en utilisant IP. Ainsi, les trames seront affichées par Wireshark de cette façon : [Malformed Packet: GSM over IP], ce qui n'est pas vrai vu que l'application ne communique pas avec ce protocole. Vous pouvez, sur Wireshark, désactiver cette association automatique en allant sur: Edit→preferences→protocols→GSM over IP → retirer le port 5000 de la liste d'association de TCP/UDP.

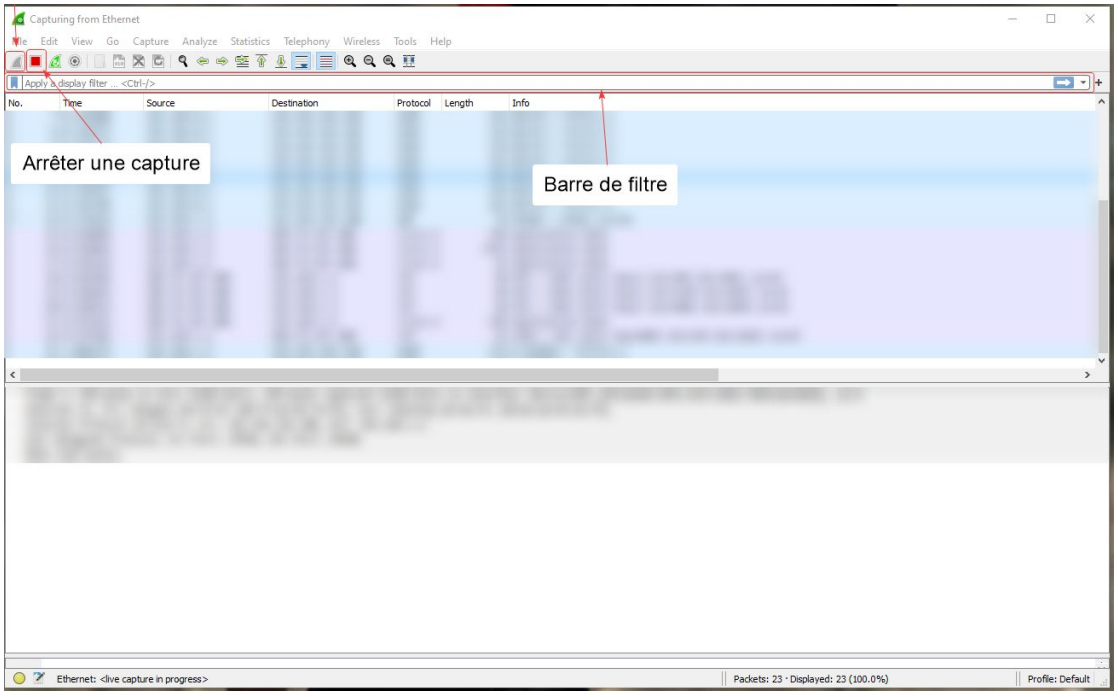
7. Comment démarrer une capture WireShark

A. Exécuter WireShark en **tant qu'administrateur**

B. Une fenêtre contenant les différentes interfaces de votre ordinateur devrait s'afficher comme suit:



C. La capture de WireShark devrait maintenant démarrer, vous pouvez l'arrêter en cliquant sur le bouton d'arrêt rouge sur la barre d'outil en haut à gauche



8. Analyse de l'application client/serveur du laboratoire 1 (10 points)

A) Lancement des applications client/serveur:

Cette partie du laboratoire consiste à analyser une application de traitement d'image. Nous vous demandons d'analyser l'application fournie sur Moodle et nommée "Traitement Sobel". Sur moodle, téléchargez le fichier "serveur_traitement_image.zip" et extrayez son contenu dans un dossier nommé "**serveur**". En gardant le bouton "*Shift"* enfoncé, faites un clic droit dans la fenêtre du "**serveur**" contenant le fichier précédemment téléchargé. Sélectionnez l'option "*Open command window here*". Ce laboratoire se fera de façon local, ainsi l'adresse IPv4 que vous utiliserez pour vous connecter au serveur est **127.0.0.1**. Lancez le premier serveur avec la commande "java -jar serveur_traitement_image.jar". Dans la console, saisissez l'adresse **127.0.0.1** et spécifiez un port d'écoute dans l'intervalle [5000, 5050]. Si une fenêtre du pare-feu s'affiche, cliquez sur "*Allow access*". Le serveur d'images devrait démarrer et être prêt à traiter les images reçues.

Vous devez maintenant démarrer le client "client_traitement_image.jar" après l'avoir téléchargé à partir de Moodle. **Assurez-vous, de démarrer la capture Wireshark avant que le client soit lancé.** Lancez le client avec la commande "java -jar client_traitement_image.jar". Entrez **127.0.0.1** comme addresse IP du serveur. Vous devez spécifier le port d'écoute sélectionné au lancement du serveur. Vous devez aussi saisir un nom d'utilisateur et un mot de passe quelconques. Lorsque le nom de l'image à traiter vous est demandé entrez "polyImage.jpg". Vous pouvez spécifier n'importe quel nom pour l'image traitée qui sera reçue (e.g. polyImageFiltree.jpg). Une fois la demande de traitement envoyée, attendez jusqu'à la réception de l'image traitée et arrêtez la capture Wireshark. Vous pouvez à présent commencer votre analyse en répondant aux questions.

B) Conseils pratiques:

Il est possible d'appliquer sur Wireshark des filtres afin de visualiser uniquement les paquets servant à la communication entre un client et le serveur. Vous pouvez vous référer à ce lien afin d'en comprendre le fonctionnement: https://wiki.wireshark.org/DisplayFilters. Ainsi, vous pouvez visualiser, par exemple, uniquement des paquets provenant de l'adresse IP du client et acheminés vers l'adresse IP du serveur. Notez que vous pouvez aussi filtrer l'affichage des paquets pour un port spécifique.

Pour analyser le flot de données entre le client et le serveur, il est possible de sélectionner un paquet de la communication et d'effectuer un clic droit et de sélectionner l'option "*Follow*

TCP/UDP/SSL Stream" en fonction du type de protocole utilisé par la couche 4. Dans la fenêtre qui s'affiche, il est possible de visualiser toutes les données qui ont transigé entre le client et le serveur. Il vous est même possible de sélectionner la direction du flot de données et de préciser le type d'affichage (*ASCII, EBCDIC, Hex Dump, C Arrays, Raw*)

Le flot de données que vous allez analyser contient une image de format jpeg. L'entête d'un fichier .jpg, en hexadécimale, commence par FF D8 FF E0 et se termine toujours par FF D9. Il est possible, avec l'outil WinHex, de modifier les données d'un fichier. Par exemple, pour supprimer des données en trop, il vous suffit d'ouvrir le fichier avec WinHex[1], de sélectionner les octets non désirés et de les supprimer avec la touche "*delete (Suppr.)*". Une fois le fichier modifié, il est possible de le sauvegarder sous un nouveau nom et avec une extension souhaitée.

C) Analyse du flot de données de l'application "Traitement Sobel"

5.2 Appliquer un outil d'ingénierie

Critère d'évaluation : Utilisation adéquate de l'outil Wireshark afin de récupérer les données et produire des résultats.

1) Quel filtre appliqueriez-vous afin d'afficher uniquement les échanges entre le client et le serveur? **(1 point)**
2) À la lumière de vos observations, dites quel protocole de la couche 4 est utilisé pour la communication entre le client et le serveur. **(0.5 point)**
3) Combien de paquets et d'octets de données ont été envoyés du client vers le serveur et du serveur vers le client? **(2 points)**

[1] http://www.x-ways.net/winhex.zip

3.5 Analyser les résultats expérimentaux

Critère d'évaluation : Qualité et exhaustivité de l'analyse des résultats obtenus à l'aide de l'outil Wireshark. L'étudiant devra rechercher, identifier et trier l'information pertinente obtenue par l'outil. À la lumière de ses résultats, il devra formuler des conclusions.

4) Normalement, le standard IEEE 802.3 limite la taille d'une trame *Ethernet* à 1518 octets. Dans votre capture Wireshark, existe-t-il des paquets ayant une taille supérieure à 1518 octets? Si oui, expliquez pourquoi et comment ce paquet réussit à transiger sur le réseau alors que sa taille est plus grande que celle spécifiée par le standard. **(2.5 points)**
5) Quel type d'information êtes-vous capables d'extraire de Wireshark en lien avec l'authentification au serveur de traitement d'images? **(1 point)**

2.2 Explorer des approches de résolution et planifier la démarche

Critère d'évaluation : Choisir un modèle ou une méthode pour analyser ou résoudre un problème, incluant les notions, les concepts ou les relations physiques pour identifier des pistes de solution

6) Il est possible, avec Wireshark, d'extraire l'image envoyée par le client ou l'image traitée. Donnez les étapes à suivre, incluant des captures d'écran montrant chaque étape permettant l'extraction de l'image envoyée du client vers le serveur. Servez-vous des propriétés du fichier .jpg énoncées plus haut. Indice: utilisez le programme *WinHex* après avoir sauvegardé le flot de données en format "*Raw*" **(2 points)**

9.4 Évaluer les risques et les incertitudes d'une situation

Critère d'évaluation : Expliquer la relation étroite entre le développement technologique et le développement social, incluant les impacts de la technologie sur la société et vice versa.

7) Suite à toute cette analyse que pouvez-vous conclure quant à la sécurité de l'application de traitement d'images que vous avez développé lors du travail pratique no.2 **(1 point)**

9. Analyse d'une application client-serveur "secrète" (10 points)

A) Lancement des applications client/serveur

Cette partie du laboratoire consiste à analyser les exécutables "secret" qui vous ont été fournis. Il faut d'abord lancer les serveurs "Server_secret_1" et "Server_secret_2". Ouvrez le dossier où vous avez sauvegardé les exécutables serveurs que vous avez téléchargés précédemment sur votre poste à partir de Moodle. En gardant le bouton "*Shift"* enfoncé, faites un clic droit dans la fenêtre du dossier. Sélectionner l'option "*Open command window here*". Lancez le premier serveur avec la commande "Server_secret_1.exe" dans la console et entrez l'adresse IPv4 **127.0.0.1**. Si une fenêtre du pare-feu s'affiche, cliquez sur "*Allow access*". Le serveur secret 1 devrait démarrer. Démarrez maintenant le second serveur "Server_secret_2.exe" de la même façon.

Vous pouvez démarrer le client "Client_secret.exe" en ouvrant une console comme décrit précédemment, il suffit de l'avoir téléchargé à partir de Moodle. Entrez l'adresse IPv4 **127.0.0.1**. **Assurez-vous, au niveau du serveur, de démarrer la capture Wireshark avant que le client lance le mode "secret".** Une fois un des modes "secrets" lancé, vous pouvez arrêter la capture Wireshark et commencer votre analyse. Pour les modes "secrets" ultérieurs, vous pouvez les lancer de la même façon et redémarrer une nouvelle capture.

B) Mode secret (1, 2, 3 et 4) (2 points chaque)

Pour chaque mode secret, pour chaque question, veuillez fournir des captures d'écran de votre analyse.

3.6. Vérifier les hypothèses et argumenter

Critère d'évaluation : Interpréter les résultats en tenant compte du contexte et des hypothèses de travail en vue de formuler des conclusions valides

1) Quel protocole de la couche transport est utilisé? Dans le cas de TCP, montrer le tout premier échange entre le client et le serveur lors de l'initialisation de la connexion, comment ce nomme cet échange? Dans le cas d'UDP, est-ce que ce même échange à lieu? Pourquoi? **(0.5 point)**
2) En vous basant sur les informations recueillies par Wireshark, indiquez les ports source et destination utilisés par la couche 4. **(0.5 point)**
3) Combien de paquets et d'octets contenant des données ont été envoyés par le client vers le serveur? Par le serveur vers le client? Montrer où vous avez trouvé cette information. **(0.5 point)**

4) À la lumière de votre analyse, que fait le client? Selon vous, combien d'itérations le client a-t-il faites pour envoyer ces données? **(0.5 point)**

C) Analyse des performances et protocole TCP (2 points)

1) Comparez la performance des envois de données pour le mode 1 et le mode 2. Qu'est-ce qui diffère entre ces deux modes? Lequel est le plus performant selon vous et pourquoi? **(0.5 point)**
2) Comparer la performance des envois de données pour le mode 3 et le mode 4. Qu'est-ce qui diffère entre ces deux modes? Lequel est le plus performant selon vous et pourquoi? **(0.5 point)**
3) Discutez de la fiabilité de chaque mode. Selon vous, quel(s) mode(s) est le plus fiable? **(0.5 point)**
4) Pour les modes secrets utilisant le protocole TCP, vous avez certainement remarqué à la fin de la communication un échange FIN, ACK. Expliquez en quoi consiste cet échange. **(0.5 point)**

10. Remise

Soumission du rapport en format PDF par moodle uniquement, contenant les réponses et des captures d'écran justifiant vos manipulations.

Annexe A

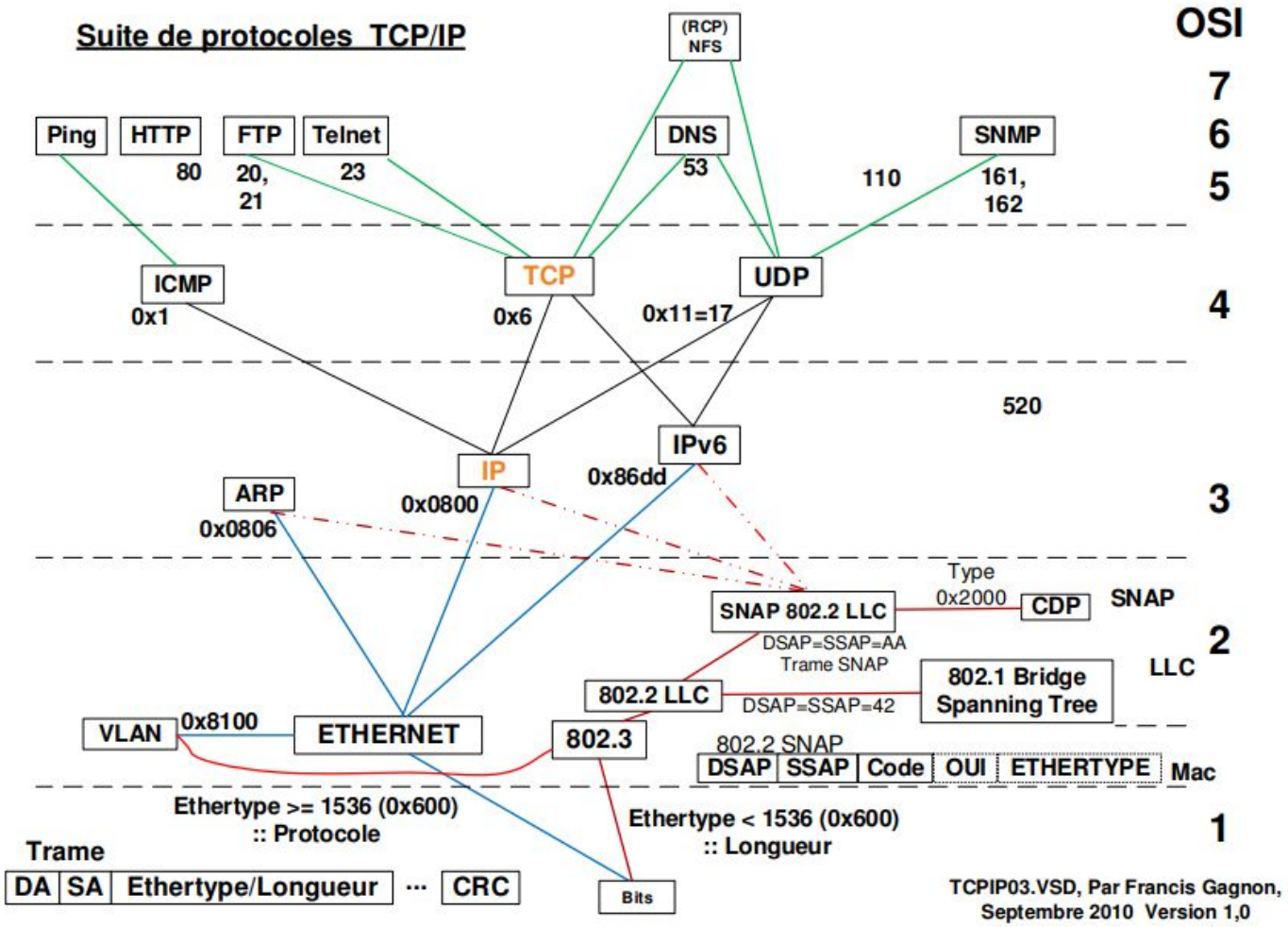


Fig.1 : Modèle OSI