INF4032 – Réseaux IP Rappels TCP/IP



Lancez le logiciel Wireshark (Rappel : pour pouvoir sniffer les paquets réseau, vous devez disposer des droits d’administration sur le système, et par conséquent, il est nécessaire que Wireshark soit lui aussi lancé en admin), sélectionnez l’interface ethY sur laquelle vous avez mis l’adresse IP et commencez une capture. Appliquez le filtre suivant : arp.

Graphical user interface, table

Description automatically generated

Grâce à la commande arp, affichez l’état de votre table ARP. Essayez de supprimer l’entrée présente. Donnez la commande utilisée dans votre rapport. Puis, faites un ping vers un poste voisin. Stoppez votre ping.

Text

Description automatically generated with medium confidence

Text

Description automatically generated

Text

Description automatically generated

Grâce au ping nous nous pouvons obtenir l’adresse mac du voisin.

A travers le ping on force le pc voisin a envoyer l’adresse mac.

2.1 Questions

1. Expliquez ce que vous observez et faites un schéma des échanges ARP qui se sont produits suite à ce ping.

Table

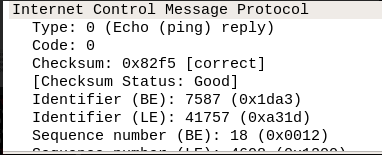
Description automatically generatedon voit bien le protocole icmp et arp.

2. Affichez votre table ARP. Qu’est-ce qui a été modifié ? Détaillez ces modifications

A screenshot of a computer

Description automatically generated with medium confidenceOn peut l’adresse ip et mac du poste voisin qui a était enregistrer dans la table arp fait précédemment.

Modifiez le filtre dans Wireshark pour mettre icmp. Pour répondre à ces questions, préciser le type de paquet ICMP que vous étudiez



2.2 Questions

1. Dans la partie Ethernet, qu’est-ce que le champ Type ? Quelle est sa valeur et à quoi sert-il ?

EtherType est un champ d'une trame Ethernet indiquant quel est le protocole de niveau supérieur utilisé dans le champ "donnée" de cette trame.

Quelque valeurs

0x0800 : IPv4

0x86DD : IPv6

0x0806 : ARP

2. Dans la partie IP, qu’est-ce que le champ Flags ? Quels sont les flags et quelles sont les valeurs

Le champ Flags est codé sur 3 bits et indique l’état de la fragmentation.

Les valeurs pour le champs flags :

0x00 NULL

0x01 FIN

0x02 SYN

0x03 FIN-SYN

3. Dans la partie IP, qu’est-ce que le champ Protocole ? Quelle est sa valeur et à quoi sert-il ?

Le champ Protocole est codé sur 8 bits et représente le type de Data qui se trouve derrière l’entête IP. Vous trouverez tous les détails des types de protocole dans la RFC 1700 qui remplace désormais la RFC 1340. Voici la liste des protocoles les plus connu :

01 – 00001 – ICMP

02 – 00010 – IGMP

06 – 00110 – TCP

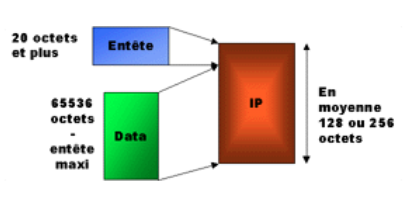
17 – 10001 – UDP

4. En vous basant sur un exemple, détaillez la structure d’un paquet IP.

Le paquet IP est formé de deux grandes parties :

l’entête du paquet, généralement d’une taille de 20 octets, constitue le PCI du protocole. C’est là que sont inscrites toutes les informations du protocole (adresse, segmentation, options, etc.).

la partie « data », ou champ de données, d’une taille maximum de : (65536 octets) – (les octets d’entête et d’options). Elle véhicule la PDU de couche supérieure (généralement un segment TCP ou UDP).



5. Dans la partie ICMP, qu’est-ce que le champ Type ? Quelle est sa valeur et à quoi sert-il ?

6. Dans la partie ICMP, qu’est-ce que le champ Code ? Quelle est sa valeur et à quoi sert-il ?

Les champs Type et Code sont codés respectivement sur 8 bits ce qui donne un totale de 2 octets. Ils représentent la définition de message d’erreur contenu. Voici la liste des principales combinaison entre les champs Type et Code :

type=00 et code=00 : Réponse à une demande d’écho

type=03 et code=00 : Réseau inaccessible

type=03 et code=01 : Hôte inaccessible

Graphical user interface, application, table

Description automatically generated7. Observez la partie data du protocole ICMP. Que remarquez-vous ?

La trame a une taille maximale et minimal à respecter pour que la donnée puisse être envoyer. Lors l’un ping il n’a pas d’échange de données, on est obligé faire du bourrage pour atteindre le seul pour que la donnée puisse être envoyer.

2.3 Questions

1. Observez la partie data du protocole ICMP. Que remarquez-vous ? On notera que cette capture a été réalisée entre deux machines Windows

2.4 Questions

1. Que pouvez-vous en déduire ? Peut-on connaître le système d’exploitation utilisé à partir d’un simple ping ?

Le ping sert à vérifier s’il y a une connexion avec un autre pc.

Donc avec le ping on ne peut pas connaitre le système d’exploitation.

En réalisant un man ping sur votre système Linux, trouvez l’option pour envoyer des messages avec cette commande.

Oui, on peut envoyer des messages avec la commande ping, d’après le manuel :

A screenshot of a computer

Description automatically generated with low confidence

2.5 Questions

1. Définissez une grammaire avec un de vos voisins connue uniquement de vous pour échanger des messages entre vous. Relancez une capture avec Wireshark et envoyez-vous des messages. Expliquez en quelques lignes votre grammaire.

Voici la commande pour envoyer le message :

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generatedcapture sur wireshark :

La grammaire de notre message signifie « hi here »

D’après le site : https://stackoverflow.com/questions/31857419/how-to-send-a-message-with-ping

3. Est-ce que vous pouvez vous faire passer pour un système Windows ? Détaillez votre réponse.

Oui on peut se faire passe pour un utilisateur Windows , si on changes les valeurs par défaut de ceux de Windows.

3 Raccordement à Internet

3.1 Questions 1.

Pouvez-vous atteindre le site http://www.cnrs.fr avec votre navigateur web ? Pourquoi ?

Oui, on peut se connecter au site, car on a une configuration automatique.

Le dns est configurer automatiquement.

3.2 Questions

1. Détaillez toutes les étapes nécessaires à la connexion sur le site. (Sous la forme d’un schéma détaillé)

Dans un premier temps, le client envoi la requête au site exemple, [www.google.com](http://www.google.com), le navigateur va lire et l’analyser le protocole, puis il va découper l’adresse en deux parties, la partie hôte et la partie page demander.

La partie hôte c’est l’endroit où sont stocker les données.

Le navigateur sait quel serveur contacter mais il ne sait où il se trouve, pour cela on utilise le protocole DNS qui permet de trouver l’adresse IP à partir de l’hôte.

Le navigateur va donc demander aux systèmes d’exploitation quel serveur DNS il doit consulter puis faire sa requête.

Le navigateur connait l’hôte, la page demandée et l’adresse IP à contacter. Il a tout ce qu’il lui faut pour établir la connexion au niveau TCP.

Après tout dépend de la requête, si c’est une requête de type GET, on demande une page web.

Dans la requête http Il indique l’Host c’est à dire à quelle machine il s’adresse, car dans un même serveur il peut avoir plusieurs sites, c’est grâce à l’entête on sait quel site est demander.

Voici le résumer pour se connecter à un site web

1) Parser la requête

2) Résolution DNS

3) Connexion au serveur WEB

4) Requête http

5) Génération de la page web

6) Réponse http

7) Parser la page web

8) Afficher la page

2. Qu’est-ce qu’une requête DNS ? Que contient une réponse DNS ?

Un DNS permet de résoudre les noms de domaine en adresses IP.

Table

Description automatically generatedVoici d’après cette capture le contenu d’une réponse DNS.

3.3 Questions

1. Sur un schéma, détaillez les three-handshaking de la connexion TCP en insistant sur les drapeaux mis en jeu (ou activés)

A picture containing timeline

Description automatically generated

le client souhaitant établir la connexion au serveur envoie un paquet ou segment SYN ,portant un numéro séquentiel aléatoire individuel. Ce numéro garantit la transmission intégrale et dans le bon ordre (sans doublons) des données.

le serveur reçoit le segment, il approuve la connexion en renvoyant un paquet SYN-ACK ,ainsi que le numéro séquentiel du client augmenté de 1. Il transmet également aux clients son propre numéro séquentiel.

le client confirme la réception du segment SYN-ACK en envoyant son propre paquet ACK qui, cette fois-ci, contient le numéro séquentiel du serveur augmenté de 1. Simultanément, il peut transmettre ses premières données au serveur.

2. Même question mais cette fois-ci en se concentrant sur la fin de la connexion.