TP Simulateur réseau

**PHASE 1 :**

***Mise en place du réseau domestique***

On met en place le réseau tel que décrit : On place deux PC connectés à un routeur Linksys par wifi. On ajoute alors un serveur, connecté lui par câble fast ethernet. On connecte ce câble à la prise « Ethernet 1 » du routeur.



On va fixer l’ip du serveur à 192 .168.1.100 manuellement :



Nous devons ensuite tester la communication. Pour cela, nous allons faire un ping à partir de PC1, vers PC0, par l’invite de commande simulée. PC0 a comme IP 192.168.1.101, et PC1 a pour IP 192.168.1.102. Quant à lui, le routeur Linksys a pour IP 192 .168.1.1.



On voit que le PC12 répond au PC0, ce qui prouve que les deux pc peuvent communiquer. Testons avec un PC et le serveur. PC0 va faire un ping vers le serveur, et cela confirme que les machines communiquent :



**PHASE 2 :**

***Configurer le réseau WIFI***

Nous allons maintenant configurer les paramètres wifi du routeur. On ouvre un navigateur à partir de PC0, et on tape l’adresse 192.168.1.1 :



Les identifiants sont admin/admin. Nous arrivons alors sur l’interface de paramétrage Linksys :



On clique sur wireless, puis on fixe le SSID à « GERANTET ». On laisse les autres paramètres sur les valeurs par défaut :



On fixe une clé wep dans l’onglet *Wireless Security*, et on rentre la clé *00AABBCCDD*.



Ensuite, dans Basic Setup, on fixe l’adresse IP de départ du DHCP à 192.128.1.70, et le nombre maximal d’utilisateurs à 10. L’adresse maximale sera alors 192.168.1.80.



Maintenant, les deux PC ne sont plus connectés avec le routeur car le SSID n’est plus valide. On met à jour le SSID et la clé wep du PC0, afin qu’il corresponde aux nouveaux réglages du routeur :



On voit ensuite que l’on est bien connecté au routeur, avec le nouveau SSID *GERANTET* et que l’on a une nouvelle IP correspondante aux limites fixées sur le routeur :



On fait de même sur PC1, et on teste un ping entre ces deux postes, pour vérifier que les connexions sont correctes. On envoie un ping de PC1 à PC0 qui confirme que tout marche bien. Les nouvelles IP sont donc 192.168.1.71 pour PC0, et 192.168.1.72 pour PC1 :



**Phase 3 :**

***Analyses de trames DHCP, ARP, ICMP et HTTP.***

Nous allons utiliser la méthode 2, ou méthode *add simple PDU*. Pour l’illustrer, nous allons créer une écoute entre PC0 et PC1 en cliquant sur *Add simple PDU* puis en cliquant sur PC0 et PC1. Il suffit ensuite de cliquer sur *Auto Capture*, et sur *Edit Filters¸*pour choisir quels informations on veut filtrer.



***Explication d’un échange DHCP :***

* Trame DHCP Discover :
Le client DHCP qui désire avoir une adresse IP va envoyer une trame DHCP Discover. Le Client ne connait pas le serveur DHCP, et de toute façon, il ne fait partie d’aucun réseau, puisqu’il n’a pas encore pas d’IP. Il va donc envoyer une trame en *Full Broadcast*: c'est-à-dire que la trame aura pour destinataire 255.255.255.255, soit un broadcast sur TOUS les réseaux. Il cherche en fait un serveur DHCP désespérément. L’adresse source sera 0.0.0.0. C’est une adresse qui signifie que le client est d’un réseau non défini, avec une IP non définie. Quant à l’adresse MAC destination, elle sera du type FFFF.FFFF.FFFF.FFFF, car au niveau IP, les trames sont envoyées en *Full Broadcast*, pour tous les échanges suivants, il en sera de même.
* Trame DHCP Offer :
Les serveurs DHCP qui vont recevoir cette trame *DHCP Discover*, vont envoyer une trame *DHCP Offer*, à destination du client en demande. Ils ne feront cet envoi qu’à condition qu’ils aient des adresses libres à distribuer. Si il leur reste des adresses à attribuer, ils enverront cette adresse au client, pour lui proposer (ils lui font une offre) cette ip.
* Trame DHCP Request :
Le client va alors recevoir 0, 1, ou plusieurs trames *DHCP Offer*, et il lui suffira de choisir laquelle il préfère. Généralement, le client va choisir la première réponse qu’il reçoit. Il va envoyer cette trame à 255.255.255.255 avec une source de 0.0.0.0. En effet, il ne fait toujours pas partie du réseau qu’il a choisi, tant que le DHCP ne l’a pas accepté, et par conséquent il n’a toujours pas d’adresse IP. De plus, il est obligé de faire un *Full Broadcast* pour être sûr de toucher le serveur DHCP qui lui a fait cette offre.
* Trame DHCP Pack :
Le serveur DHCP qui a fait l’offre saura se reconnaitre. Si un serveur qui a fait une offre reçoit une trame *DHCP Request* qui ne correspond pas à l’offre qu’il a faite, cette trame sera ignorée. Sinon, le serveur DHCP va prendre en compte la requête, et attribuer l’IP préalablement proposée au client. Il ne proposera plus cette IP, tant que le bail d’attribution sera valable. Il doit alors prévenir le client que sa requête a été acceptée, et que l’IP lui a été attribuée. Il va donc lui envoyer une trame *DHCP Pack* pour lui dire quelle IP lui a été attribuée.

Remarque : Si le client est redémarré, il ne refera pas toutes les étapes pour obtenir son adresse, il renverra seulement la *DHCP Request*. Si l’adresse qui lui avait précédemment été attribuée n’est plus libre, il refera toutes les étapes.

***Explication d’un échange ARP :***

ARP sert à faire le lien entre les adresses IP et les adresses MAC. Si il manque une entrée dans une table ARP, des échanges ARP vont être engagés sur le réseau, pour combler ce trou, et savoir qui cette IP identifie :

* Demande ARP :
Tout d’abord, si une entrée est vide dans la table ARP, et que l’on veut envoyer une trame IP à une adresse IP, il nous faut trouver l’adresse MAC de la machine correspondante. Ainsi, la machine va tout d’abord envoyer une trame ARP avec comme adresse mac une adresse de broadcast FFFF.FFFF.FFFF.FFFF et cette trame est envoyée en broadcast IP sur le réseau.
* Réponse ARP :
Seul le destinataire de la requête ARP saura se reconnaitre, ainsi il répondra à la machine à l’origine de la demande ARP. Les adresses IP et MAC de la machine à l’origine de la demande sont comprises dans sa demande. La machine qui va répondre va mettre son adresse MAC en source, et son adresse IP en source aussi. La machine demandeuse aura alors toutes les informations qu’elle demandait.
* Réception de la réponse :
A la réception de la réponse ARP, la machine qui avait fait la demande va mettre à jour sa table ARP, afin de pouvoir communiquer avec la machine dont elle ne connaissait que l’IP auparavant. L’adresse MAC de cette dernière est en source de la réponse.

*Remarque :* Comme la demande ARP a été faite en broadcast IP, toutes les machines ont reçu cette demande (mais ils ne l’ont pas traité puisque cela ne les concernait pas). Ainsi, toutes les machines ont reçu un message venant d’une IP, avec son adresse MAC. Toutes les machines qui n’auraient pas cette IP dans leur table ARP, ou dont l’adresse MAC ne correspondrait pas avec l’IP prévue, vont mettre à jour elles aussi leur table ARP. A noter que la réponse n’étant pas envoyé en broadcast, les autres machines du réseau ne sauront pas obligatoirement l’adresse MAC de la machine ciblée par la demande.

Pour illustrer cet échange, nous avons fait une demande ARP depuis un PC vers la Box. Observons que les tables ARP de PC1, mais aussi de PC0 ont été mises à jour :

*Table ARP du PC-PT-PC1 mise à jour*



*Table ARP du PC-PT-PC0 mise à jour (192.168.1.1 correspond à la Box)*



***Explication d’un échange ICMP :***

Les échanges ICMP ont pour but de contrôler le bon fonctionnement d’un réseau. Le principe est simple : à une demande, contenant un message « echo », une machine répondra par un « replay ».

Cet échange assez simpliste nous permet de contrôler que deux machines peuvent communiquer sans soucis ensembles…

Ici dans l’exemple, nous allons utiliser la commande ping pour envoyer une trame ICMP. L’identifiant permet d’identifier la commande ping par un numéro. Le numéro de séquence permettra alors de mettre en relation l’echo et le replay, pour réorganiser les échanges.

***Explication d’un échange HTML :***

Les échanges HTML mettent en relation un client HTML et un serveur HTML.
Le niveau d’encapsulation de HTML est le 7, soit la couche Application.
La couche Transport utilisé par le protocole http est TCP. En effet, UDP ne fait aucun cntrole sur l’intégrité des données, hors HTML est un protocole qui doit faire parvenir les informations intactes.
Le numéro de port utilisé pour la destination est le 80 (C’est un WKP).
Le numéro de port utilisé pour la source est le 1027.
Le port client est donc le 1027 et le port serveur est donc le 80.

**Phase 4 :**

***Construire et configurer le réseau du FAI.***

On commence par mettre en place le réseau sous Packet Tracer (voir Fichier de phase 4) :

