TP 2 : Analyse de protocoles

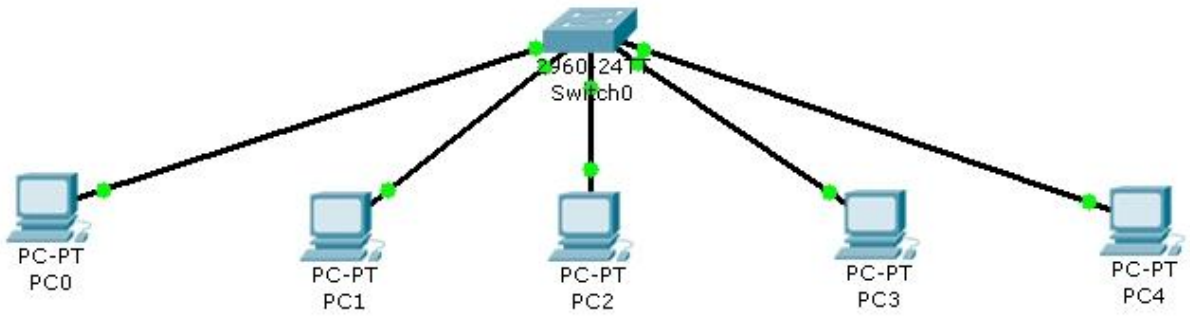
Matière: **RESEAUX LOCAUX** Enseignant: Ramzi BELLAZREG

Objectif du TP

Au cours de ce TP, nous allons simuler des cas de communications et voir en détail les différentes étapes de la communication. Vous allez observez en détail, le mécanisme de l'encapsulation au niveau de tout les nœuds qui participent dans la communication. Vous allez aussi voir comment les paquets et trames sont organisés pour différencier les différents types de flux (ARP request ou reply, echo request ou reply, http, dns ….).

La simulation se fera en mode PDU, pour voir les différents paquets qui circulent de point de vue temporel.

Scénario 1 : Analyse de protocole ARP et ICMP



- La topologie à utiliser tout au long de ce TP comporte 5 postes et un switch de type 2960 ;
- Commencer par attribuer des adresses IP aux différents postes ;

Passer en mode simulation PDU. Lancer un ping du poste PC0 vers le poste PC4. Laisser la simulation se poursuivre jusqu'à ce que la réponse complète à la commande ping soit reçue.

Faites un filtre pour n'afficher que les paquets ARP et ICMP.

I - La requête ARP

On considère en premier lieu la requête ARP lancée par PC0.

1) Pourquoi une requête ARP a été lancée avant que la requête « echo request » ne soit envoyée ?
2) Est-ce que la requête ARP est encapsulée dans un paquet IP ? Le protocole ARP est un protocole de quelle couche ?
3) Quels sont les différents champs de la trame? Et quelle est la signification de chacun de ces champs ?
4) Quelle est la différence entre le datagramme ARP et la trame Ethernet ?
5) Identifier l'adresse MAC source et destination. Pourquoi la requête ARP a été envoyée en diffusion ?

6) Au niveau de l'unité de donnée ARP, Identifier l'adresse IP source et destination ? Au niveau de la question 2, nous avons vu que la requête ARP n'est pas encapsulée dans un paquet IP mais directement dans une trame. Quelle est donc la signification des adresses logiques ?
7) Expliquer comment un poste arrive à détecter que la trame reçue encapsule des datagrammes ARP ? Indiquer le champ et sa valeur.
8) On considère le même champ de la question 7. Quelle est l'utilité de ce champ ? Faites une recherche et mentionner les différentes valeurs que peut prendre ce champ.
9) Une fois que le poste a identifié qu'il s'agit du protocole ARP, comment le processus ARP détecte que c'est une requête (indiquer le champ utilisé et sa valeur) ;
10) Est-ce que la requête contient des numéros de ports source et destination. Commentez.
11) Expliquer le mécanisme de décapsulation détaillé quand un poste reçoit une trame qui contient un protocole ARP ? Comment un poste décide que c'est lui qui doit répondre à la requête ARP.

II - La réponse ARP

On considère dans cette partie la réponse ARP envoyée par PC4.

1) Identifier l'adresse MAC source et destination. Pourquoi la réponse n'est pas envoyée en diffusion tel que la requête ARP ;
2) Est-ce que la réponse ARP est encapsulée dans paquet IP ?
3) Expliquer comment un poste arrive à détecter que les trames capturées encapsulent des datagrammes ARP et en particulier une réponse qui lui est destinée ;
4) Quel est le résultat retourné par une réponse ARP ? Où se trouve l'information au niveau du datagramme ARP.

III - La requête echo request (ping sortant)

On considère dans cette partie la requête ICMP « ping sortant ».

1) Identifier l'adresse MAC source et destination ;
2) Identifier l'adresse IP source et destination ;
3) Quelle est la valeur du champ Type ? Quelle est sa signification ?
4) Après réception du signal sur la couche physique, comment le poste (carte réseau) détecte que la trame lui est destinée ?
5) Une fois que la poste a accepté la trame, quelles sont les taches qu'il fait ?
6) Comment le poste détecte qu'un paquet IP est encapsulé dans la trame ?
7) Dans un paquet IP peuvent être encapsulées des datagrammes correspondant à plusieurs types de protocoles ? Quel est le champ qui indique le type de protocole encapsulé dans le paquet IP ?
8) Comment le PC détecte que le datagramme encapsulé dans le paquet est de type ICMP ?
9) Une fois que le poste a détecté que le flux est de type ICMP. Quels sont les champs et leurs valeurs qui permettent de détecter que c'est en particulier un « echo request » ;
10) Quel est le nombre de trames générées par la commande « ping » ? Montrer qu'il est cohérent avec ce qui a été affiché lors de l'exécution de la commande ;
11) Quelle est la valeur TTL des paquets relatifs aux requêtes ICMP ? Quelle est la signification de ce champ.

IV - La réponse echo reply

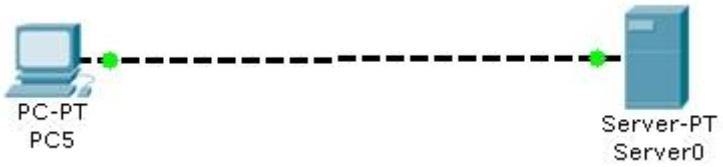
1) Identifier l'adresse MAC source et destination ;
2) Identifier l'adresse IP source et destination ;
3) Expliquer comment un poste arrive à détecter qu'il s'agit d'un message ICMP de type echo reply encapsulé dans un paquet IP, qui est lui aussi encapsulé dans une trame Ethernet. Quels sont les champs indicateurs et leurs valeurs ;

V – Lors de l'arrivée d'une trame sur le port du commutateur, comment celui là agit. Dans votre réponse présenter la procédure d'encapsulation et décapsulation ;

VI - Lancer un deuxième ping du poste PC0 vers le poste PC4. Est-ce que la requête ICMP a été précédée par une requête ARP. Expliquer ?

Scénario 2 : Analyse de protocole DNS et HTTP

- Dans cette partie, nous allons utiliser un poste et un serveur (http + DNS).



- Commencer par attribuer des adresses IP à PC5 et au serveur ;
- Au niveau du serveur DNS, ajouter le nom de domaine www.RI3.tn à l'adresse IP que vous avez attribué au serveur.

A partir du navigateur du poste PC5, demander le site www.RI3.tn. Laisser la simulation se poursuivre jusqu'à ce que la page demandée soit affichée au niveau du navigateur.

I - Décrivez l'ordre et les différents types des paquets qui transitent depuis la demande du site jusqu'à l'affichage de la page. Expliquer le rôle de chacun d'eux ;

II - Respectivement pour la requête DNS et la réponse DNS, voir en détails :

1) Les champs les plus importants des datagrammes ;
2) Comment se fait l'ordre l'encapsulation ;
3) Quel est le protocole de transport utilisé et comment vous avez fait pour l'identifier ;
4) Les numéros de ports source et destination ;
5) Les adresses IP et MAC ;

III – L'établissement de connexion en trois étapes

1) Dans cette étape, vous allez suivre l'établissement de la connexion TCP en *3 way hand shake* avant le début de l'échange des données HTTP. Il faut mentionner comment les valeurs des Flags SYN et ACK sont positionnées au cours de cet échange ;
2) Pourquoi une requête ARP n'est pas précédée par un établissement de connexion entre émetteur et récepteur.

IV - Respectivement pour la requête http et la réponse http, examiner en détail :

1) Les champs les plus importants des datagrammes ;
2) Comment se fait l'ordre d'encapsulation ;
3) Quel est le protocole de transport utilisé ;

4) Les numéros de ports source et destination ;
5) Les adresses IP et MAC source et destination;
6) Le suivi des acquittements envoyés, en termes de valeurs des champs numéro de séquence et ACK ;