Réseau CR tp2

1. apr –a –d (vidage table arp)

Dans la trame ethernet type indique ARP (photo 1)

2) après le type dans la zone data (photo1 partie surlignée) padding 18 bytes + 28 bytes ARP = 46 soit minimum data

3)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hardware  Type (2bytes) | Protocol  Type  (2bytes) | Hardware  Size (1byte) | Protocol  Size  (1 byte) | Opcode  Request (0001) or reply (0002)  2 bytes | @ Mac emetteur  6bytes | @ IP  Emetteur  4bytes | @ Mac recepteur  6bytes | @ IP  recepteur  4bytes |

Protocol d’en dessous : Ethernet

Protocol du dessus : IP => historique pour être universel, mais toujours utilisation ethernet/IP

Résolution d’adresse ethernet en adresse IP

Voir photo pour code binaire

4) le niveau ethernet ne connait pas la taille des paquets, il ne le connait pas non plus (marqueur de fin)

Octets de bourrage correspondent à la partie padding : placer après arp

5) Toute la couche données est transmise = protocol arp + bourrage

6)

tantque vrai faire

attendre(evenement)

• si evenement est “Question sur adresse internet” (requete interne de IP vers ARP)

...

finsi

• si evenement est expiration du timer d’effacement associe à une entree

...

finsi

• si evenement est reception requete (ARP Request)

...

finsi

• ... (attention il y a d’autres evenements)

fin tantque

7) La machine B enregistre l’adresse ethernet de la machine A lors de la requette arp de A vers B. cela economise une requete.

8) Un paquet iCMP envoyé par A vers B, puis une requete ARP de B vers A soit un ARP request de B vers A et un arp reply de A vers B. Car A connait l’adresse de B dans sa table ARP mais plus B car suppression.

Info : timer arp 1200 seconde soit 20 minutes.

9) C’est le timer de ping : 1 seconde . ARP envois juste un paquet pour demander l’adresse, si pas trouvé pas de reemission.

On peut tester avec un envoi d’un seul paquet par le ping : ping –c on constate qu’il y a un seul paquet arp envoyé.

10) lors de la configuration d’une interface, un paquet arp gratuit est envoyé sur le reseau. Un paquet arp gratuit est un paquet arp envoyé en broadcast (ethernet) avec l’adresse IP de la machine ajoutée sur le reseau. Aucune reponse si pas de conflit IP. Si l’adresse IP utilisée par la machine ajoutée est déjà utilisée par une autre machine, cette dernière va envoyé un message comme quoi cette adresse est déjà utilisé.

11) Deux paquet ARP reply sont envoyé. En effet lors d’un ping de C vers B, la machine C envoit un ARP request vers B. B recoit ce paquet et répond avec un ARP reply. Cependant, la machine A possède la correspondance adresse IP et adresse Ethernet de B en published dans sa table. La clause published autorise alors A a répondre au ARP request envoyé par C. Il y a donc à l’issu de ce ping deux paquets ARP reply :

* Paquet envoyé par Machine B : source ethernet Machine B, source ARP Machine B
* Paquet envoyé par Machine A : source ethernet Machine A, source ARP Machine B

On remarque que les adresse Ethernet source de ces deux paquets correspondent à l’adresse de la machine émétrice, cependant l’adresse source au niveau de la trame ARP est dans les deux cas l’adresse de la machine B, celle visée initiallement par le ARP request.

12) Il est possible de déclarer en published une association IP Ethernet/IP dans la table ARP afin de récuperer des paquets qui ne nous sont pas destinés. En effet, lors de l’envoi d’un paquet, une machine quelquonque envoie un paquet ARP request, et la machine destination va répondre avec un ARP reply. Ensuite (il faut que se soit après le paquet ARP reply de la machine destination pour écraser l’association dans la table ARP) la machine pirate va repondre au ARP request en associant l’adresse IP de destination avec sa propre adresse Ethernet. Cela écrase donc la première association dans la table ARP de la machine source. Au prochain envoie d’un paquet, l’adresse Ethernet associée à l’adresse IP de destination sera donc l’adresse de la machine pirate.

13) Lors de la configuration d’une machine avec une adresse IP correspondant à une adresse IP déjà utilisée sur le reseau, un message d’alerte est affiché sur les deux machines correspondantes. Ce message indique que l’adresse IP est déjà utilisé ou que une machine tiers vient d’utiliser cette adresse pour configurer une de ses interface. Il correspond à un conflit d’IP sur le reseau :

Lors de la configuration de l’interface, un ARP gratuit est envoyé sur le reseau. Si une machine possède déjà cette adresse IP, un message d’alerte s’affiche sur sa console et elle envoie en réponse un ARP gratuit à destination de la machine « voleuse » pour la prévenir et llui faire afficher le message d’alerte.

14) La machine emetrice du paquet ICMP va envoyer une requete ARP, les deux machines avec la même adresse IP vont répondre en donnant leur adresse ethernet. La premiere qui repond se voit retourner un paquet icmp (ping) mais le reply de la deuxieme machine ecrase dans la table arp de la machine qui ping l’adresse ethernet de la premiere machine. Ainsi, les paquet icmp du ping suivant seront tous redirigés vers la deuxieme machine.

Au bout de 20 minutes, le timer à zero va reemettre une requete ARP, ainsi, on relance les dès pour savoir qui va recevoir les paquets icmp. En effet c’est toujours la machine qui répond en dernier qui « gagne ».

15) Ils sont identiques entre request et reply, et correspondent bien à ceux envoyés (dans le fichier texte).

Pour un ping, ils sont identiques entre une request et un reply pour cette request. Pour un même ping, identifier reste le même pour toutes les requetes et sequence number s’incrémente à chaque requète, identifiant ainsi le numèros de la requete pour le ping (processus) donné.

16) complement a 1, verifier WireShark Q 16 pour le deuxieme paquets :

x08 00 00000000

Ce type de vérification permet de mettre en évidence des érreures en séquences ( bits éronnés qui se suivent ) mais des erreures isolées (situé alors sur la même colonne pour le calcule) de nombre paire ( si erreures en nombre impare on peut les detecter) seront indecelables.

# DHCP :

17) Un paquet DHCP request est envoyé par notre machine. En brodcast 255…… Un paquet DHCP ACK est alors envoyé par le routeur par deffaut avec son adresse IP et notre adresse IP a untiliser sur ce reseau et eventuellement le nom du reseau (pas dans notre cas).

Dans notre cas, il n’y a pas de difference de l’interface apres un dhclient em0 car il y a un adressage par defffaut avec une adresse.

Fragmentation

18) Dans le cas de l’envoi d’un paquet de 4600 bytes :

Envoi de quatre paquets :

Un premier paquet IP avec un identifiant n , une taille 1500(data+enteteIP) et un flag more fragment et un fragment offset à 0.

Un deuxieme paquet IP avec un identifiant n , une taille 1500 et un flag more fragment et un fragment offset à 1480.

Un troisieme paquet IP avec un identifiant n , une taille 1500 et un flag more fragment(x01) et un fragment offset à 2960.

Un paquet UDP, avec en IP un identifiant n , une taille 188(data+entete IP + entete UDP) et un flag x00 fragment et un fragment offset à 4440. Dans la trame udp, il y a la taille total du paquet non framenté de 4608 (data + entete UDP)

UDP sur le dernier paquet car c’est en réalité un seul gros paquet UDP. IP rassemble du premier au derni avec entete