Réseaux : Analyse requête http.

1. TCP, DNS, http
2. dns.qry.name=="manpages.org" **ou** dns contains « manpages »
3. IP SRC: 192.168.254.5 | MAC SRC: 00 :0c :29: d3: 0e: 2c
4. Protocole IPv4 (0x0800)
5. IP DEST : 1.1.1.1 | MAC DEST : 00 :50 :56 :f0 :5f :a1
6. L’adresse MAC du DEST correspond à la *default gateway*, la passerelle par défaut. L’IP correspond au DNS SEVREUR de Google.
7. Taille header IP = 20 octets. Taille totale (IP+TCP/UDP+APPLICAT°) = 58 octets.
8. Le protocole de la couche transport est l’UDP.
9. Le port UDP SRC = 48651 et le port UDP DEST = 53. Le port SRC change pour toute machine, le port DEST 53 signifie que la couche application est du DNS.
10. La longueur de l’entête UDP = 38 octets. Cela correspond bien car paquet IP = 58o total et donc les 58o – les 20o (header IP) = 38o.
11. Le champs *flag*: si le bit est à 0 = requête, si à 1 = réponse.
12. Type A (renseigne IPv4, si « AAAA » alors IPv6), classe IN.
13. Transaction ID : 0x7cf6.
14. IP SRC: 1.1.1.1 | MAC SRC: 00 :50 :56: f0 :5f: a1

IP DEST: 192.168.254.5 | MAC DEST: 00 :0c :29: d3: 0e: 2c

1. Le header IP vaut toujours 20o, mais la taille du paquet vaut 106o. C’est parce que la réponse DNS se trouve dans le champs DATA.
2. L’identificateur de la transaction est 0x7cf6 et oui il correspond.
3. Il y a 3 réponses. Le TTL correspond au temps de vie d’un paquet sur le réseau.

|  |  |  |  |
| --- | --- | --- | --- |
| Application | DNS | Donnée/data |  |
| Transport | UDP | Segment | Port 53 |
| Internet | IP | Paquet |  |
| Accès réseau | Ethernet | Frame/trame |  |

1. IP SRC: 192.168.254.5 | MAC SRC: 00 :0c :29: d3: 0e: 2c

IP DEST: 172.67.151.202 | MAC DEST: 00 :50 :56: f0 :5f: a1

TCP, IPv4

1. Port SRC : 39820 port DEST : 80 (http). Le port SRC est > 1024 donc dynamique.
2. N° seq = 2951767386 (= 0 en relatif) et MSS = 1460 octets
3. Synchronisation des numéros de séquence afin d’établir une connexion.
4. N° seq = 3049732393 (0 en relatif). MSS = 1460o
5. SYN signifie demande de synchronisation et ACK signifie qu’on a bien reçu la demande.
6. Car lors de l’acquittement, le numéro est incrémenté de 1 afin de dire qu’on peut passer au segment suivant.
7. L’indicateur ACK du client indique la connexion est établie.
8. La connexion est établie.



Une image contenant texte

Description générée automatiquement

1. N° seq 2951767387 (1 relatif) et ACK = 3049732394 (1 relatif)
2. Push et ack pour envoyer la requête http
3. Entête = 20o et requête 323o
4. /
5. Next seq n° = 3049732394