L3 Informatique

Système d’exploitation - Devoir maison

Serveur DNS

Table des matières

[1 – Synthèse RFC1035 3](#_Toc467584526)

[1.1 – Message 3](#_Toc467584527)

[1.2 – En-tête 3](#_Toc467584528)

[1.3 – Question 4](#_Toc467584529)

[1.4 – Enregistrement de ressource 5](#_Toc467584530)

[1.5 – Compression de message 5](#_Toc467584531)

[1.6 – Transport 6](#_Toc467584532)

[1.6.1 – UDP 6](#_Toc467584533)

[1.6.2 – TCP 6](#_Toc467584534)

[2 – Analyse d’une trace Wireshark (exemples\_dns.pcapng) 7](#_Toc467584535)

[2.1 - Paquet n°1 : 7](#_Toc467584536)

[2.2 - Paquet n°2 : 8](#_Toc467584537)

[2.3 - Paquet n°3 : 9](#_Toc467584538)

# 1 – Synthèse RFC1035

Tous les tableaux ci-dessous sont découpés en 16 colonnes (une pour chaque bit).

## 1.1 – Message

Chaque message (question et réponse) suit le même format :

|  |
| --- |
| En-tête |
| Question (pour le serveur de nom) |
| Réponse (de la part des enregistrements de ressources) |
| Autorité (désignée par les enregistrements de ressources) |
| Section additionnelle (de la part des enregistrements de ressources) |

## 1.2 – En-tête

L’en-tête est de la forme :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | | | | | | | |
| QR | OPCODE (4 bits) | AA | TC | RD | RA | Z (3 bits à 0) | RCODE (4 bits) |
| QDCOUNT | | | | | | | |
| ANCOUNT | | | | | | | |
| NSCOUNT | | | | | | | |
| ARCOUNT | | | | | | | |

Où :

ID : L’identifiant de la requête. Il est le même pour la question et la réponse (pour pouvoir les coupler).

QR : Type de message. 0 pour une question et 1 pour une réponse.

OPCODE : Nature de la requête. Définie par la question et réutilisée par la réponse. Les valeurs utilisées sont 0 pour une requête standard, 1 pour une requête inversée et 2 pour une requête de statut.

AA : Utilisé pour la réponse, vaut 1 si le premier serveur qui répond est une autorité pour le domaine demandé, 0 sinon.

TC : Indique si le message a été tronqué.

RD : Utilisé par la question, indique si la question veut une réponse récursivement au niveau des serveurs de noms.

RA : Utilisé par la réponse, indique si le serveur de noms supporte les questions récursives.

RCODE : Code de réponse.

0 – Pas d’erreur  
1 – Erreur de format  
2 – Faute de serveur  
3 – Erreur de nom (le nom de domaine est introuvable par le serveur autoritaire)  
4 – Non implémenté (cette requête n’est pas supportée par le serveur)  
5 – Refusé (pas d’information sur le demandeur par exemple)  
6-15 – Réservés pour usages ultérieurs

QDCOUNT : Nombre d’entrées dans la section Question

ANCOUNT : Nombre d’enregistrements de ressources dans la section Réponse

NSCOUNT : Nombre de serveurs de noms dans la section autorité

ARCOUNT : Nombre d’enregistrements de ressources dans la section Additionnelle

## 1.3 – Question

La section Question est de la forme :

|  |
| --- |
| QNAME (nom de domaine) |
| QTYPE (type de la requête) |
| QCLASS (classe de la requête, IN pour internet par exemple) |

QNAME : Suite de labels qui décrivent le nom de domaine. Un label est composé d’un octet qui indique la taille d’une chaîne de caractères (qui décrit le sous-domaine) puis un à un les caractères de cette chaîne. Un label a obligatoirement ses deux bits de poids fort à 0. La suite se termine par un octet à 0 (pour la racine).

Par exemple, pour le nom de domaine info.unicaen.fr, la sous-section QNAME est de la forme :

|  |  |
| --- | --- |
| 4 | I |
| N | F |
| O | 7 |
| U | N |
| I | C |
| A | E |
| N | 2 |
| F | R |
| 0 | (la racine n’a pas de label) |

## 1.4 – Enregistrement de ressource

Les sections Réponse, Autorité et Additionnelle ont toutes le même format :

|  |
| --- |
| NAME |
| TYPE |
| CLASS |
| TTL |
| RDLENGTH |
| RDATA |

NAME : le nom de domaine auquel est rattaché l’enregistrement.

TYPE : Le type des données de la sous-section RDATA

CLASS : La classe des données dans la sous-section RDATA

TTL : Un entier non signé sur 32 bits qui indique si le serveur qui manipule le message doit garder les informations dans sa cache. Chaque serveur décrémente cet entier et un entier à 0 signifie la fin du message.

RDLENGTH : La taille de la sous-section RDATA exprimée en octets.

RDATA : Une chaîne d’octets qui représente la ressource.

## 1.5 – Compression de message

Pour limiter la taille des messages, lorsqu’un nom de domaine est déjà présent dans la section QNAME, on ajoute un label avec ses deux bits de poids fort à 1 et on écrit l’offset où trouver ce domaine dans l’octet suivant.

Par exemple, pour les noms de domaine unicaen.fr et info.unicaen.fr, cela donne :

|  |  |
| --- | --- |
| 7 | U |
| N | I |
| C | A |
| E | N |
| 2 | F |
| R | 4 |
| I | N |
| F | O |
| 11000000 | 20 |
| 0 |  |

## 1.6 – Transport

Les messages peuvent être échangés en utilisant le protocole UDP (port 53) ou le protocole TCP (port 53).

### 1.6.1 – UDP

Les messages UDP sont restreints à 512 octets (hors en-têtes IP et UDP). Les messages plus longs sont tronqués.

Aux vues des particularités d’UDP, certaines précautions sont recommandées à l’utilisateur :

- le client devrait essayer différents serveurs et noms de serveur avant de répéter sa requête à la même adresse de serveur ;  
 - la retransmission minimum est conseillée entre 2 et 5 secondes.

### 1.6.2 – TCP

Le message est préfixé par un mot de deux octets indiquant la taille du message (moins ce mot).

Une politique de gestion de connexion est recommandée :

- le serveur ne devrait pas arrêter ses activités dans l’attentes des données TCP ;  
 - le serveur devrait supporter plusieurs connexions ;  
 - le serveur devrait assumer que le client demandera la fin de la connexion. Il devrait donc maintenir sa partie de la connexion jusqu’à la fin de la transmission des données demandées par le client ;  
 - si le serveur devrait fermer une connexion dormante, il est conseillé d’attendre 2 minutes avant.

# 2 – Analyse d’une trace Wireshark (exemples\_dns.pcapng)

Dans tous les tableaux ci-dessous, une case représente un octet du paquet (la valeur de cette case est exprimée en hexadécimal).

## 2.1 - Paquet n°1 :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 52 | 54 | 00 | 12 | 35 | 02 | 08 | 00 |
| 27 | 06 | 53 | 79 | 08 | 00 | 45 | 00 |
| 00 | 3C | 8B | E4 | 40 | 00 | 40 | 11 |
| 18 | 34 | 0A | 00 | 02 | 0F | 0A | 0E |
| 80 | 7D | 8B | 21 | 00 | 35 | 00 | 28 |
| 96 | D3 | 92 | CB | 01 | 00 | 00 | 01 |
| 00 | 00 | 00 | 00 | 00 | 00 | 03 | 64 |
| 6E | 73 | 07 | 75 | 6E | 69 | 63 | 61 |
| 65 | 6E | 02 | 66 | 72 | 00 | 00 | 01 |
| 00 | 01 |  |  |  |  |  |  |

ETHERNET :

* Octets de 0 à 5 : Adresse destination = 52 :54 :00 :12 :35 :02
* Octets de 6 à 11 : Adresse source = 08 :00 :27 :06 :53 :79
* Octets de 12 à 13 : Type = IPv4

IP :

* Octet 14 : Protocole IPv4, taille de l’en-tête = 20 octets
* Octet 15 : Type de service
* Octets 16 à 17 : Taille du paquet (en-tête IP + contenu) = 60 octets
* Octets 18 à 19 : ID = 0x8BE3
* Octets 20 à 21 : Fragmentation = ne pas fragmenter
* Octet 22 : Time To Live = 64
* Octet 23 : Protocole = UDP
* Octets 24 à 25 : Checksum de l’en-tête = 0x1834
* Octets 26 à 29 : Adresse source = 10.0.2.15
* Octets 30 à 33 : Adresse destination = 10.14.128.125

UDP :

* Octets 34 à 35 : Port source = 36509
* Octets 36 à 37 : Port destination = 53
* Octets 38 à 39 : Taille du paquet (en-tête UDP + contenu) = 40
* Octets 40 à 41 : Checksum = 0x96D3

DNS :

En-tête

* Octets 42 à 43 : ID de la transaction = 0x92CB
* Octets 44 à 45 : QR à 0, OPCODE à 0, AR à 0, TC à 0, RD à 1, RA à 0, Z à 0 et RCODE à 0 (cf. 1.2)
* Octets 46 à 47 : QDCOUNT à 1
* Octets 48 à 49 : ANCOUNT à 0
* Octets 50 à 51 : NSCOUNT à 0
* Octets 52 à 53 : ARCOUNT à 0

Section Question

* Octets 54 à 69 : QNAME = dns.unicaen.fr
* Octets 70 à 71 : QTYPE = A
* Octets 72 à 73 : QCLASS = IN

## 2.2 - Paquet n°2 :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 52 | 54 | 00 | 12 | 35 | 02 | 08 | 00 |
| 27 | 06 | 53 | 79 | 08 | 00 | 45 | 00 |
| 00 | 3C | 8B | E4 | 40 | 00 | 40 | 11 |
| 18 | 33 | 0A | 00 | 02 | 0F | 0A | 0E |
| 80 | 7D | 8B | 21 | 00 | 35 | 00 | 28 |
| 96 | D3 | 84 | C0 | 01 | 00 | 00 | 01 |
| 00 | 00 | 00 | 00 | 00 | 00 | 03 | 64 |
| 6E | 73 | 07 | 75 | 6E | 69 | 63 | 61 |
| 65 | 6E | 02 | 66 | 72 | 00 | 00 | 1C |
| 00 | 01 |  |  |  |  |  |  |

ETHERNET :

* Octets de 0 à 5 : Adresse destination = 52 :54 :00 :12 :35 :02
* Octets de 6 à 11 : Adresse source = 08 :00 :27 :06 :53 :79
* Octets de 12 à 13 : Type = IPv4

IP :

* Octet 14 : Protocole IPv4, taille de l’en-tête = 20 octets
* Octet 15 : Type de service
* Octets 16 à 17 : Taille du paquet (en-tête IP + contenu) = 60 octets
* Octets 18 à 19 : ID = 0x8BE4
* Octets 20 à 21 : Fragmentation = ne pas fragmenter
* Octet 22 : Time To Live = 64
* Octet 23 : Protocole = UDP
* Octets 24 à 25 : Checksum de l’en-tête = 0x1833
* Octets 26 à 29 : Adresse source = 10.0.2.15
* Octets 30 à 33 : Adresse destination = 10.14.128.125

UDP :

* Octets 34 à 35 : Port source = 36517
* Octets 36 à 37 : Port destination = 53
* Octets 38 à 39 : Taille du paquet (en-tête UDP + contenu) = 40
* Octets 40 à 41 : Checksum = 0x96D3

DNS :

En-tête

* Octets 42 à 43 : ID de la transaction = 0x84C0
* Octets 44 à 45 : QR à 0, OPCODE à 0, AR à 0, TC à 0, RD à 1, RA à 0, Z à 0 et RCODE à 0 (cf. 1.2)
* Octets 46 à 47 : QDCOUNT à 1
* Octets 48 à 49 : ANCOUNT à 0
* Octets 50 à 51 : NSCOUNT à 0
* Octets 52 à 53 : ARCOUNT à 0

Section Question

* Octets 54 à 69 : QNAME = dns.unicaen.fr
* Octets 70 à 71 : QTYPE = AAAA
* Octets 72 à 73 : QCLASS = IN

## 2.3 - Paquet n°3 :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 08 | 00 | 27 | 06 | 53 | 79 | 52 | 54 |
| 00 | 12 | 35 | 02 | 08 | 00 | 45 | 00 |
| 00 | 6A | F2 | 27 | 00 | 00 | 40 | 11 |
| F1 | C1 | 0A | 0E | 80 | 7D | 0A | 00 |
| 02 | 0F | 00 | 35 | 8B | 21 | 00 | 56 |
| FD | 2D | 84 | C0 | 85 | 00 | 01 | 00 |
| 00 | 00 | 00 | 01 | 00 | 00 | 03 | 64 |
| 6E | 73 | 07 | 75 | 6E | 69 | 63 | 61 |
| 65 | 6E | 02 | 66 | 72 | 00 | 00 | 1C |
| 00 | 01 | C0 | 10 | 00 | 06 | 00 | 01 |
| 00 | 01 | 51 | 80 | 00 | 22 | 09 | 64 |
| 6E | 73 | 6D | 61 | 73 | 74 | 65 | 72 |
| C0 | 10 | C0 | 2C | 78 | 2B | 48 | C9 |
| 00 | 01 | 51 | 81 | 00 | 00 | 0E | 10 |
| 00 | 36 | EE | 80 | 00 | 01 | 51 | 80 |

ETHERNET :

* Octets de 0 à 5 : Adresse destination = 08 :00 :27 :06 :53 :79
* Octets de 6 à 11 : Adresse source = 52 :54 :00 :12 :35 :02
* Octets de 12 à 13 : Type = IPv4

IP :

* Octet 14 : Protocole IPv4, taille de l’en-tête = 20 octets
* Octet 15 : Type de service
* Octets 16 à 17 : Taille du paquet (en-tête IP + contenu) = 106 octets
* Octets 18 à 19 : ID = 0xF227
* Octets 20 à 21 : Fragmentation = 0x0000
* Octet 22 : Time To Live = 64
* Octet 23 : Protocole = UDP
* Octets 24 à 25 : Checksum de l’en-tête = 0xF1C1
* Octets 26 à 29 : Adresse source = 10.14.128.125
* Octets 30 à 33 : Adresse destination = 10.0.2.15

UDP :

* Octets 34 à 35 : Port source = 53
* Octets 36 à 37 : Port destination = 36517
* Octets 38 à 39 : Taille du paquet (en-tête UDP + contenu) = 86
* Octets 40 à 41 : Checksum = 0xFD2D

DNS :

En-tête

* Octets 42 à 43 : ID de la transaction = 0x84C0
* Octets 44 à 45 : QR à 1, OPCODE à 0, AR à 1, TC à 0, RD à 1, RA à 1, Z à 0 et RCODE à 0 (cf. 1.2)
* Octets 46 à 47 : QDCOUNT à 1
* Octets 48 à 49 : ANCOUNT à 0
* Octets 50 à 51 : NSCOUNT à 1
* Octets 52 à 53 : ARCOUNT à 0

Section Question

* Octets 54 à 69 : QNAME = dns.unicaen.fr
* Octets 70 à 71 : QTYPE = AAAA
* Octets 72 à 73 : QCLASS = IN

Section Autorité

* Octets 74 à 75 : NAME = 0xC010 (référence à unicaen.fr)
* Octets 76 à 77 : TYPE = SOA
* Octets 78 à 79 : CLASS = IN
* Octets 80 à 83 : TTL = 0x00015180 (86400 en base 10)
* Octets 84 à 85 : RDLENGTH = 34
* Octets 86 à 119 : RDATA =
  + (86-97) Serveur de nom principal : dnsmaster.unicaen.fr (cf. 1.5)
  + (98-99) Boîte mail : dnsmaster.unicaen.fr
  + (100-103) Numéro de série : 2016102601
  + (104-107) Intervalle de rafraîchissement : 1 jour et 1 seconde
  + (108-111) Intervalle avant nouvel essai : 1 heure
  + (112-115) Limite d’expiration : 41 jours et 16 heures
  + (116-119) TTL minimum : 1 jour