TD2 Couche application

1 DNS

Exercice 1. Après avoir rappelé rapidement le principe du service de gestion de noms DNS (on n'oubliera pas la résolution inverse), représentez graphiquement l'espace des noms, les sous-domaines et les autorités.

Exercice 2. Les serveurs DNS et le protocole DNS participent à la mise en oeuvre de la politique de gestion des noms. Analysez le contenu de la table 1. Quelle différence entre le serveur DNS fourni par le FAI et les autres serveurs contactés dans cette table ?

Exercice 3. Pourquoi une politique de gestion de cache est-elle nécessaire au bon fonctionnement du DNS ? Où peut-on trouver un cache DNS et quel est l'intérêt de chaque emplacement ? En supposant que, parti d'un cache vide, on a effectué les requêtes de la table 1, représentez les informations contenues dans les différents niveaux de cache. Quelles requêtes va-t-on effectuer pour résoudre `www.apple.com` ?

Exercice 4. Le protocole DNS est la mise en oeuvre réseau des échanges participant à la résolution DNS. Analysez les messages DNS de la table 2 à l'aide des annexes.

Exercice 5. Tous ces aspects techniques cachent des règles politico-commerciales nécessaires à la mise en oeuvre effective du DNS à l'échelle de l'internet. Vous êtes chargé d'installer un serveur web qui fournira la page web accessible à l'URL http://www.supercalifragilisticexpialidocious.com/. Quels sont les impératifs techniques ?

2 SMTP

Exercice 6. Vous souhaitez envoyer un email à l'adresse `m.delacourt@dim.uchile.cl`. À quel serveur SMTP faut-il se connecter pour transmettre ce message ? En pratique, comment votre client de messagerie envoie-t-il le message ? Pourquoi ?

Exercice 7. Analysez la session SMTP de la table 3. Déduisez-en une séance typique d'échanges avec un serveur SMTP. Expliquez comment utiliser ce protocole pour gérer correctement les champs `To:`, `Cc:` et `Cci:` (ou `Bcc:`).

Exercice 8. Le message reçu correspondant à la session de la question précédente est reproduit sur la table 4. En déduire le trajet effectué par ce message. À quoi les entêtes `Return-Path:` et `Delivered-To:` servent-elles ?

Exercice 9. Le courrier électronique permet-il tel quel d'assurer l'authenticité des messages ? l'identité de l'expéditeur ? Pour autant permet-il vraiment l'émission anonyme de messages ?

3 HTTP

Exercice 10. Expliquez comment s'interprète une URI et en déduire les étapes que doit suivre un client web pour accéder à l'URI `http://maps.google.fr/maps?q=turku&z=12`. Précisez la requête HTTP envoyée par le client au serveur.

serveur consulté	*question*	*type*	*classe*	*réponse*	*type*	*classe*
FAI	www.perdu.com.	A	IN	82.165.176.145	A	IN
FAI	145.176.165.82.in-addr.arpa.	PTR	IN	u15184286.onlinehome-server.com.	PTR	IN
A.ROOT-SERVERS.NET	www.perdu.com.	A	IN	com. → A.GTLD-SERVERS.NET.	NS	IN
				A.GTLD-SERVERS.NET. → 192.5.6.30	A	IN
A.GTLD-SERVERS.NET	www.perdu.com.	A	IN	perdu.com. → ns.bok.net.	NS	IN
				ns.bok.net. → 82.165.176.145	A	IN
ns.bok.net	www.perdu.com.	A	IN	82.165.176.145	A	IN
A.ROOT-SERVERS.NET	145.176.165.82.in-addr.arpa.	PTR	IN	82.in-addr.arpa. → NS3.NIC.FR.	NS	IN
NS3.NIC.FR	145.176.165.82.in-addr.arpa.	PTR	IN	165.82.in-addr.arpa. → ns.ripe.net.	NS	IN
				ns.ripe.net. → 193.0.0.193	A	IN
ns.ripe.net	145.176.165.82.in-addr.arpa.	PTR	IN	176.165.82.in-addr.arpa. → nsa.schlund.de.	NS	IN
nsa.schlund.de.	145.176.165.82.in-addr.arpa.	PTR	IN	u15184286.onlinehome-server.com.	PTR	IN

TABLE 1 – Requêtes et réponses DNS

```
0000  d4 c3 01 00 00 01 00 00 00 00 00 00 03 77 77 77  .............www
0010  05 70 65 72 64 75 03 63 6f 6d 00 00 01 00 01     .perdu.com.....


0000  d4 c3 81 80 00 01 00 01 00 00 00 00 03 77 77 77  .............www
0010  05 70 65 72 64 75 03 63 6f 6d 00 00 01 00 01 c0  .perdu.com......
0020  0c 00 01 00 01 00 00 1a ad 00 04 52 a5 b0 91     ...........R...


0000  a0 c7 01 00 00 01 00 00 00 00 00 00 03 31 34 35  .............145
0010  03 31 37 36 03 31 36 35 02 38 32 07 69 6e 2d 61  .176.165.82.in-a
0020  64 64 72 04 61 72 70 61 00 00 0c 00 01           ddr.arpa.....


0000  a0 c7 81 80 00 01 00 01 00 00 00 00 03 31 34 35  .............145
0010  03 31 37 36 03 31 36 35 02 38 32 07 69 6e 2d 61  .176.165.82.in-a
0020  64 64 72 04 61 72 70 61 00 00 0c 00 01 c0 0c 00  ddr.arpa........
0030  0c 00 01 00 01 51 80 00 21 09 75 31 35 31 38 34  .....Q..!.u15184
0040  32 38 36 11 6f 6e 6c 69 6e 65 68 6f 6d 65 2d 73  286.onlinehome-s
0050  65 72 76 65 72 03 63 6f 6d 00                    erver.com.
```

Table 2 – Messages DNS capturés

```
220 dio.univ-orleans.fr ESMTP Postfix (Debian/GNU)
HELO delu
250 dio.univ-orleans.fr
MAIL FROM: martin.delacourt@univ-orleans.fr
250 2.1.0 Ok
RCPT TO: mdelacourt@dim.uchile.cl
250 2.1.5 Ok
RCPT TO: mathieu.liedloff@univ-orleans.fr
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: martin.delacourt@univ-orleans.fr
To: mdelacourt@dim.uchile.cl
Date: Tue, 22 Oct 2019 12:12:12 +0100
Subject: Les vacances sont en vue !
C'est dans 3 jours.
M.
.
250 2.0.0 Ok: queued as EB6ED7AACE
QUIT
221 2.0.0 Bye
```

Table 3 – Exemple de session SMTP

```
Return-Path: <martin.delacourt@univ-orleans.fr>
X-Original-To: mdelacourt@dim.uchile.cl
Delivered-To: mdelacourt@dim.uchile.cl
Received: from scfilter.dim.uchile.cl (unknown [10.0.0.179])
(using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
(No client certificate requested)
by gauss.dim.uchile.cl (Postfix) with ESMTPS id A1E166EC9D
for <mdelacourt@dim.uchile.cl>; Thu, 26 Sep 2019 11:53:34 -0300 (-03)
Received: by scfilter.dim.uchile.cl (Postfix, from userid 65534)
id 46fHxB4DMbzyWF; Thu, 26 Sep 2019 11:53:34 -0300 (-03)
Received: from localhost (localhost.localdomain [127.0.0.1])
by scfilter.dim.uchile.cl (Postfix) with ESMTP id 46fHxB1643zyRx
for <mdelacourt@dim.uchile.cl>; Thu, 26 Sep 2019 11:53:34 -0300 (-03)
X-Virus-Scanned: Scrollout F1 at dim.uchile.cl
X-Spam-Flag: NO
X-Spam-Score: 2.898
X-Spam-Level: **
X-Spam-Status: No, score=2.898 tagged_above=-1000 required=5
tests=[BAYES_20=-0.001, DATE_IN_FUTURE_96_Q=2.899,
RCVD_IN_DNSWL_NONE=-0.0001, SPF_HELO_NONE=0.001, SPF_PASS=-0.001]
autolearn=no autolearn_force=no
Received: from scfilter.dim.uchile.cl ([127.0.0.1])
by localhost (scfilter.dim.uchile.cl [127.0.0.1]) (amavisd-new, port 10024)
with LMTP id Slwx7Txsf7WB for <mdelacourt@dim.uchile.cl>;
Thu, 26 Sep 2019 11:53:19 -0300 (-03)
Received: from dio.univ-orleans.fr (dio.univ-orleans.fr [194.167.30.47])
by scfilter.dim.uchile.cl (Postfix) with ESMTP id 46fHwt5yKnzyWq
for <mdelacourt@dim.uchile.cl>; Thu, 26 Sep 2019 11:53:18 -0300 (-03)
Received: from localhost (localhost [127.0.0.1])
by dio.univ-orleans.fr (Postfix) with ESMTP id 0A6C67AADB;
Thu, 26 Sep 2019 16:53:06 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at dio.univ-orleans.fr
Received: from dio.univ-orleans.fr ([127.0.0.1])
by localhost (dio.univ-orleans.fr [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id zy7PoIunhRcv; Thu, 26 Sep 2019 16:53:05 +0200 (CEST)
Received: from delu (unknown [192.168.80.22])
by dio.univ-orleans.fr (Postfix) with SMTP id EB6ED7AACE;
Thu, 26 Sep 2019 16:48:53 +0200 (CEST)
From: martin.delacourt@univ-orleans.fr
To: mdelacourt@dim.uchile.cl
Date: Tue, 22 Oct 2019 12:12:12 +0100
Subject: Les vacances sont en vue !
Message-Id: <20190926145306.0A6C67AADB@dio.univ-orleans.fr>

C'est dans 3 jours.
M.
```

TABLE 4 – Message reçu à l'arrivée

A Formats

Cet annexe résume les formats des messages DNS (RFC 1034 et 1035).

A.1 Protocole DNS

```
+---------------------+
|        Header       |
+---------------------+
|       Question      | the question for the name server
+---------------------+
|        Answer       | RRs answering the question
+---------------------+
|      Authority      | RRs pointing toward an authority
+---------------------+
|      Additional     | RRs holding additional information
+---------------------+
```

A.1.1 Header

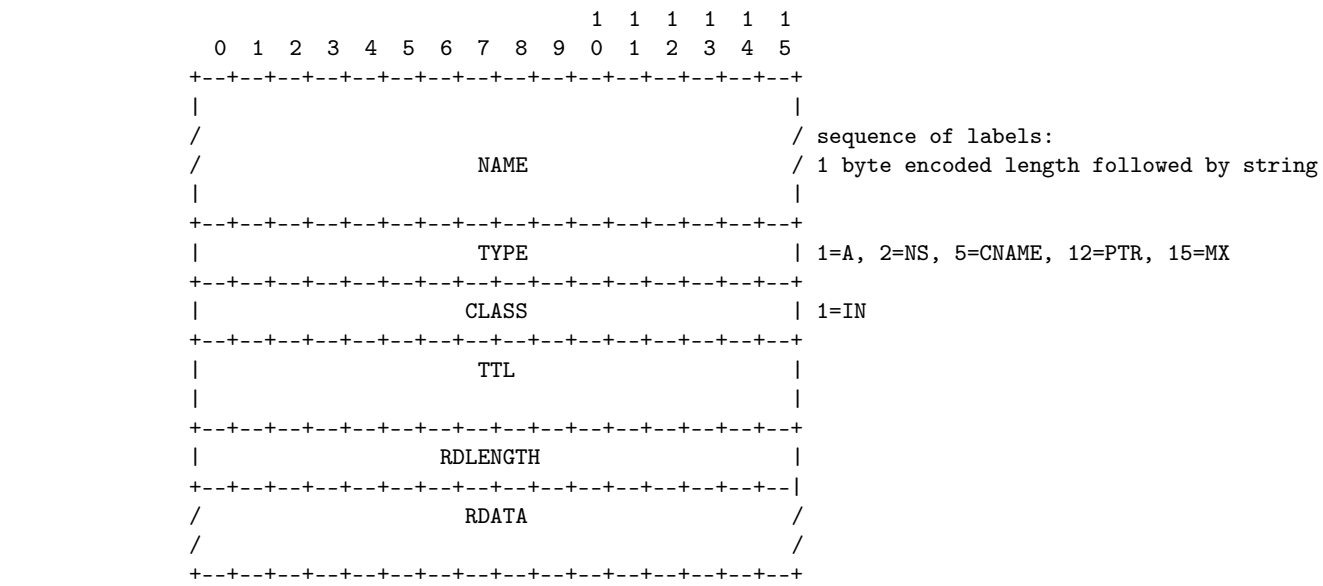
```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QDCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    NSCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

QR : query or response
Opcode: 0=QUERY, 2=STATUS
xxCOUNT: number of entries
```

A.1.2 Question

```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                               |
/                    QNAME                      / sequence of labels:
/                                               / 1 byte encoded length followed by string
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QTYPE                      | 1=A, 2=NS, 5=CNAME, 12=PTR, 15=MX
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QCLASS                     | 1=IN
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

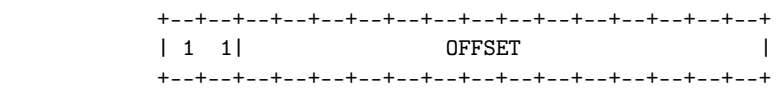
A.1.3 Resource record



A.1.4 Message compression

Les suffixes de noms de domaines répétés peuvent être compressés :

```
The pointer takes the form of a two octet sequence:
```



L'offset démarre au premier octet du champ ID dans le header.