TD 4 : ANALYSE DE TRAMES

IEEE 802.3, LLC, ETHERNET

1. IEEE 802.3

Rappel : Les trames envoyées ou reçues par un hôte représentent concrètement une suite de bits (0 et 1). Ces bits sont analysés par les entités protocolaires implantées dans l'hôte de destination. Chaque partie de cette suite binaire correspond à un entête destiné à un protocole spécifique du modèle en couche. Ainsi, la carte d'interface réseau, qui implante généralement la couche physique et éventuellement la couche liaison, récupère les premiers bits reçus et les analyse avant de remonter le restant des bits aux couches supérieures. La couche supérieure est identifiée grâce à un champ indiquant le numéro (l'identifiant) de la couche. Parfois une couche est associée uniquement à une seule couche supérieure. Dans ce cas, il n'est pas nécessaire de prévoir un champ dédié à l'identification de la couche ou de la sous-couche supérieure (c'est le cas par exemple des trames MAC de l'IEEE 802.5 - Token Ring).

Exercice :

Voici une suite de bits d'une trame entière représentée en hexadécimal (chaque lettre ou chiffre code 4 bits). Dans cette suite, on n'a pas montré le préambule du niveau physique ni le CRC du niveau MAC :

```
0180c2000000003085dd960200264242030000000000800000100b329b3b0000
00138000003085dd9607800e0100140002000f000000000000000000
```

C'est une trame MAC IEEE 802.3 qui encapsule des données LLC qui à leur tour contiennent des données du protocole STP (Spanning Tree Protocol) utilisé pour construire un arbre logique entre ponts ou commutateurs connectant des segments de LAN qui est une configuration classique de réseaux locaux. Les figures 1. et 2. donnent le format général de la trame.

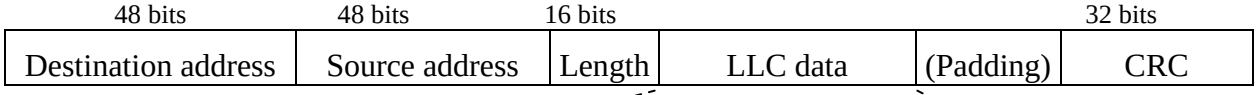

Figure 1. Encapsulation d'une trame IEEE 802.3 au niveau MAC

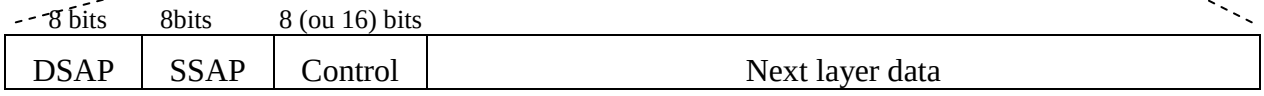

Figure 2. Format d'une trame LLC

1.1. Déterminez l'adresse MAC source et destination en hexadécimal.

1.2. Les trois premiers octets de l'adresse MAC désignent généralement le constructeur de la carte. Quel est le constructeur de la carte réseau qui a généré cette trame ? Voir Annexe.

1.3. Déterminez à quelle machine la trame est destinée ?

1.4. Déterminez la longueur des données. Y a-t-il des bits de bourrage dans cette trame ? Justifiez ?

1.5. LLC

1.5.1. Quel est le code (= numéro = identifiant = point d'accès au service = SAP) utilisé pour identifier le protocole STP ?

1.5.2. Sachant que le format du champ 'control' est le suivant :

□□□□□□□0 = trame I (Information) : transmission de messages de données numérotés

□□□□□□01 = trame S (Supervision) : fonction de contrôle comme un acquittement ou rejet

□□□□□□11 = trame U (Unnumbered) : messages de données ou de contrôle non numérotés

□ = 0 ou 1

Quel est le type de cette trame LLC ?

2. ETHERNET

Généralement, les logiciels de capture de trames captent et affichent par défaut les 68 premiers octets des trames (sans compter le préambule ni le CRC). Afin de simplifier la lecture et l'analyse, chaque groupe de 16 octets est affiché sur une ligne différente. De plus, des espaces sont insérés entre les octets ou les groupes d'octets. C'est le cas par exemple de `tcpdump` et de `wireshark`. En plus, le format de l'affichage varie selon les options de la commande.

Exercice :

Répondez aux questions suivantes en analysant ces 3 trames binaires.

```
0x0000:  0050 2282 2fb9 0004 23c3 2b52 0800 4500
0x0010:  02fc 8890 4000 4006 954b c0a8 ccc8 c0a8
0x0020:  cc06 9805 0016 032f e60f e575 415e 8018
0x0030:  05b4 9af6 0000 0101 080a 8bf1 6d79 00bb
0x0040:  154b 0000 02c4 0514 42f7 d636 f260 b617
0x0050:  1f63 db2d 6ff9 5431 0000 0059 6469 6666

0x0000:  0004 23c3 2b52 0050 2282 2fb9 0800 4500
0x0010:  0034 5402 4000 4006 cca1 c0a8 cc06 c0a8
0x0020:  ccc8 0016 9805 e575 415e 032f e8d7 8010
0x0030:  0039 a1fc 0000 0101 080a 00bb 154b 8bf1
0x0040:  6d79

0x0000:  0004 23c3 2b52 0050 2282 2fb9 0800 4500
0x0010:  0344 5403 4000 4006 c990 c0a8 cc06 c0a8
0x0020:  ccc8 0016 9805 e575 415e 032f e8d7 8018
0x0030:  0039 8119 0000 0101 080a 00bb 154b 8bf1
0x0040:  6d79 0000 030c 0a14 e3b4 a346 f9dd b955
```

2.1. Quelles sont les adresses MAC des deux machines qui échangent ces trames ?

Vous constatez qu'il n'y a pas d'entête LLC après l'Ethernet. On trouve directement l'entête IP.

2.2. Dans l'entête Ethernet, le champ ''Length'' est remplacé par le champ ''Type''. Quel est le rôle du champ ''Type'' ? Quelle la valeur qui indique que l'entête suivant est l'entête du protocole IP ? (Voir Annexe)

2.3. Comment la couche MAC de la destination peut-elle trouver la longueur des données utiles en cas de bourrage ?! Cela représente-t-il une violation du fonctionnement de l'architecture en couches ?

2.4. Comment une carte compatible Ethernet et 802.3 peut-elle distinguer entre une trame Ethernet et une trame 802.3 ?

Annexe

1. La trame Ethernet

La trame Ethernet est structurée de la façon suivante :

64 bits	48 bits	48 bits	16 bits		32 bits
Preamble (PHY layer)	Destination address	Source address	Type	Data	CRC

« Preamble » est un préambule qui détermine le début d'une trame ;

« Destination address » est l'adresse physique de destination de la trame ;

« Source address » est l'adresse physique de l'expéditeur de la trame ;

« Type » définit le type de contenu de la trame ; ainsi il est possible de déterminer quel protocole de niveau supérieur va utiliser le paquet encapsulé dans le champs « donnée » de la trame :

Type (0x)	Utilisation
0600	XEROX NS IDP
0800	DoD Internet (Datagramme IP)
0801	X.75 Internet
0802	NBS Internet
0803	ECMA Internet
0804	ChaosNet
0805	X.25 niveau 3
0806	ARP
0807	XNS
6001 à 6006	DEC
8035	RARP
8098	Appletalk

« Data » contient les données brutes de la trame à passer au protocole déterminé par le champ « type » ;

« CRC » est le checksum (code polynomial) de la trame permettant d'assurer son intégrité.

2. IEEE OUI

Le listing suivant donne la correspondance entre quelques IEEE OUI (Organizational Unique Identifier) et leur organisation (2 OUIs au maximum apparaissent ici pour chaque organisation). La liste complète peut être obtenue à partir du lien https://standards.ieee.org/products-services/regauth/oui/ de l'IEEE Registration Authority.

```
00-1C-A1   (hex)                AKAMAI TECHNOLOGIES, INC.
00-11-8B   (hex)                Alcatel-Lucent, Enterprise Business Group
00-03-93   (hex)                Apple Computer, Inc.
00-05-02   (hex)                APPLE COMPUTER
00-07-14   (hex)                Brightcom
00-01-42   (hex)                Cisco Systems, Inc.
00-30-85   (hex)                CISCO SYSTEMS, INC.
00-1A-11   (hex)                Google Inc.
00-09-2D   (hex)                HTC Corporation
00-23-76   (hex)                HTC Corporation
00-02-B3   (hex)                Intel Corporation
00-04-23   (hex)                Intel Corporation
00-05-85   (hex)                Juniper Networks, Inc.
00-10-DB   (hex)                Juniper Networks, Inc.
00-01-6B   (hex)                LightChip, Inc.
00-05-86   (hex)                Lucent Technologies
00-04-56   (hex)                Motorola PTP Inc
00-04-BD   (hex)                Motorola BCS
00-09-BF   (hex)                Nintendo Co.,Ltd.
00-16-56   (hex)                Nintendo Co., Ltd.
00-02-EE   (hex)                Nokia Danmark A/S
00-0B-E1   (hex)                Nokia NET Product Operations
00-00-75   (hex)                Nortel Networks
00-01-81   (hex)                Nortel Networks
00-10-E5   (hex)                SOLECTRON TEXAS
00-0A-D9   (hex)                Sony Ericsson Mobile Communications AB
00-0E-07   (hex)                Sony Ericsson Mobile Communications AB
00-01-2A   (hex)                Telematica Sistems Inteligente
00-01-92   (hex)                Texas Digital Systems
00-06-00   (hex)                Toshiba Teli Corporation
00-00-39   (hex)                TOSHIBA CORPORATION
00-05-69   (hex)                VMware, Inc.
00-0C-29   (hex)                VMware, Inc.
00-08-11   (hex)                VOIX Corporation
00-50-22   (hex)                Zonet Technology, Inc.
```

3. Adresses de diffusion Ethernet/802.3

Voici quelques adresses de diffusion attribuées par l'IANA (Internet Assigned Numbers Authority) et leur fonction. Une liste complète se trouve à l'adresse :
http://www.iana.org/assignments/ethernet-numbers

```
Ethernet              Type
Address               Field   Usage

Multicast Addresses:

01-00-0C-CC-CC-CC     -802-   CDP (Cisco Discovery Protocol), VTP (Virtual
Trunking Protocol)
01-00-0C-DD-DD-DD     ????    CGMP (Cisco Group Management Protocol)
01-00-10-00-00-20     -802-   Hughes Lan Systems Terminal Server S/W download
```

```
01-00-10-FF-FF-20       -802-   Hughes Lan Systems Terminal Server S/W request
01-00-1D-00-00-00       -802-   Cabletron PC-OV PC discover (on demand)
01-00-1D-42-00-00       -802-   Cabletron PC-OV Bridge discover (on demand)
01-00-1D-52-00-00       -802-   Cabletron PC-OV MMAC discover (on demand)
01-00-3C-xx-xx-xx       ????    Auspex Systems (Serverguard)
01-00-5E-00-00-00       0800    DoD Internet Multicast (RFC-1112)
through
01-00-5E-7F-FF-FF
01-00-5E-80-00-00       ????    DoD Internet reserved by IANA
through
01-00-5E-FF-FF-FF
01-00-81-00-00-00       ????    Synoptics Network Management
01-00-81-00-00-02       ????    Synoptics Network Management
01-00-81-00-01-00       -802-   (snap type 01A2) Bay Networks (Synoptics)
autodiscovery
01-00-81-00-01-01       -802-   (snap type 01A1) Bay Networks (Synoptics)
autodiscovery
01-20-25-00-00-00        873A    Control Technology Inc's Industrial Ctrl Proto.
through
01-20-25-7F-FF-FF
01-80-24-00-00-00       8582    Kalpana Etherswitch every 60 seconds
01-80-C2-00-00-00       -802-   Spanning tree (for bridges)
01-80-C2-00-00-01       -802-   802.1 alternate Spanning multicast
through
01-80-C2-00-00-0F
01-80-C2-00-00-10       -802-   Bridge Management
01-80-C2-00-00-11       -802-   Load Server
01-80-C2-00-00-12       -802-   Loadable Device
01-80-C2-00-00-14       -802-   OSI Route level 1 (within area) IS hello?
```