

Fiche Synthèse : Protocoles et réseaux

1. Mise en évidence de l'encapsulation

Avec un logiciel adapté, on a capturé les trames échangées lorsqu'un PC demande l'affichage de la page www.google.fr dans un navigateur. Les premières trames ne servent qu'à l'établissement de la connexion. La trame sélectionnée est la demande la page web en question.

The image shows a Wireshark packet capture. The top pane displays a list of packets. Packet 7 is selected, which is an HTTP GET request. The bottom pane shows the details of this packet, including the Ethernet II header, Internet Protocol (IP) header, and Hypertext Transfer Protocol (HTTP) header. The HTTP header shows a GET request for the URL 'http://www.google.fr/'. The packet is 837 bytes long.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.11	209.85.135.103	TCP	49961 > http [FIN, ACK] Seq=1 Ack=1 win=16331 Len=0
2	0.000457	192.168.1.11	74.125.43.102	TCP	49963 > http [FIN, ACK] Seq=1 Ack=1 win=16464 Len=0
3	0.000941	192.168.1.11	209.85.135.103	TCP	49965 > http [FIN, ACK] Seq=1 Ack=1 win=16921 Len=0
4	0.002284	192.168.1.11	209.85.135.103	TCP	49967 > http [FIN, ACK] Seq=1 Ack=1 win=16921 Len=0
5	0.090016	209.85.135.103	192.168.1.11	TCP	49967 > http [SYN, ACK] Seq=0 Ack=1 win=5720 Len=0 MSS=1460
6	0.090116	192.168.1.11	209.85.135.103	TCP	49967 > http [ACK] Seq=1 Ack=1 win=17040 Len=0
7	0.090374	192.168.1.11	209.85.135.103	HTTP	GET /webhp?sourceid=navclient&hl=fr&ie=UTF-8 HTTP/1.1
8	0.176054	209.85.135.103	192.168.1.11	TCP	http > 49967 [ACK] Seq=1 Ack=784 win=7047 Len=0
9	0.185746	209.85.135.103	192.168.1.11	TCP	[TCP segment of a reassembled PDU]
10	0.188735	209.85.135.103	192.168.1.11	TCP	[TCP segment of a reassembled PDU]
11	0.188775	192.168.1.11	209.85.135.103	TCP	49967 > http [ACK] Seq=784 Ack=2841 win=17040 Len=0
12	0.192037	209.85.135.103	192.168.1.11	HTTP	HTTP/1.1 200 OK (text/html)
13	0.303257	192.168.1.11	209.85.135.103	TCP	49961 > http [FIN, ACK] Seq=1 Ack=1 win=16331 Len=0
14	0.303536	192.168.1.11	74.125.43.102	TCP	49963 > http [FIN, ACK] Seq=1 Ack=1 win=16464 Len=0
15	0.303629	192.168.1.11	209.85.135.103	TCP	49965 > http [FIN, ACK] Seq=1 Ack=1 win=16921 Len=0
16	0.305607	192.168.1.11	74.125.43.102	TCP	49967 > http [SYN, ACK] Seq=0 Ack=1 win=5720 Len=0 MSS=1460
17	0.381387	192.168.1.11	209.85.135.103	TCP	49967 > http [ACK] Seq=784 Ack=3293 win=16588 Len=0
18	0.394403	74.125.43.102	192.168.1.11	TCP	http > 49969 [SYN, ACK] Seq=0 Ack=1 win=5720 Len=0 MSS=1420

Frame 7 (837 bytes on wire, 837 bytes captured)

Ethernet II, Src: SMCNetwo_6f:b7:11 (00:13:f7:6f:b7:11), Dst: SagemCom_39:f0:eb (00:60:4c:39:f0:eb)

Internet Protocol, Src: 192.168.1.11 (192.168.1.11), Dst: 209.85.135.103 (209.85.135.103)

Transmission Control Protocol, Src Port: 49967 (49967), Dst Port: http (80), Seq: 1, Ack: 1, Len: 783

Hypertext Transfer Protocol

0000 00 60 4c 39 f0 eb 00 13 f7 6f b7 11 08 00 45 00 .L9....o...E.
 0010 03 37 13 64 40 00 06 09 ed c0 a8 01 0b d1 55 .7.d@.....U
 0020 87 67 c3 2f 00 50 71 79 db 2a ab 3c 08 61 50 18 .g./..PgY*...<.ap.
 0030 42 90 dd de 00 00 47 45 54 20 2f 7f 65 62 68 70 B....GET/webhp
 0040 3f 73 6f 75 72 63 65 69 64 3d 6e 61 76 63 6c 69 ?sourceid=navcli
 0050 65 6e 74 26 68 6c 3d 66 72 26 69 65 3d 55 54 46 ent&hl=f&ie=UTF
 0060 2d 38 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 -8 HTTP/1.1.Acc
 0070 65 70 74 3a 20 69 6d 61 67 65 2f 67 69 66 2c 20 ept: image/gif,
 0080 69 6d 61 67 65 2f 78 2d 78 62 69 74 6d 61 70 2c image/x-bitmap,
 0090 20 69 6d 61 67 65 2f 6a 70 65 67 2c 20 69 6d 61 image/jpeg, ima
 00a0 67 65 2f 70 6a 70 65 67 2c 20 61 70 70 65 69 63 ge/jpeg, applic
 00b0 61 74 69 6f 6e 2f 78 2d 6d 73 2d 61 70 70 6c 69 ation/x-ms-appli
 00c0 63 61 74 69 6f 6e 2c 20 61 70 70 6c 69 63 61 74 cation, applicat
 00d0 69 6f 6e 2f 76 6e 64 2e 6d 73 2d 78 70 73 64 6f ion/vnd.ms-xpsdo

Frame (frame), 837 bytes Packets: 29 Displayed: 29 Marked: 0 Dropped: 0

En vous aidant de la capture ci-dessus, compléter le tableau suivant (modèle TCP/IP) :

Couche 1 : Accès Réseau			
@MAC Destination	@MAC Source	...	Données de la couche 2
Couche 2 : internet			
IP Source	IP Destination	...	Données de la couche 3
Couche 3 : Transport			
Port Source	Port destination	...	Données de la couche 4
Couche 4 : Application			
Protocole utilisé			

Fiche Synthèse : Protocoles et réseaux

2. Décodage de trame-1

Les deux trames suivantes ont été capturées à la suite. En vous aidant du site www.frameip.com (rubriques entêtes), décoder totalement les 2 trames

```
ff ff ff ff ff 00 13  f7 6f b7 11 08 06 00 01
08 00 06 04 00 01 00 13  f7 6f b7 11 c0 a8 01 0b
00 00 00 00 00 00 c0 a8  01 01
```

```
00 13 f7 6f b7 11 00 60  4c 39 f0 eb 08 06 00 01
08 00 06 04 00 02 00 60  4c 39 f0 eb c0 a8 01 01
00 13 f7 6f b7 11 c0 a8  01 0b 01 81 01 81 01 81
01 81 13 2f 7c d2 b4 5f 61 fb b7 74
```

Note : Préambule + SFD et FCS n'apparaissent pas ici.

Trame 1 (Ethernet)	Trame 2 (Ethernet)
<p>@MAC Destination:</p> <p>@MAC Source :</p> <p>Protocole couche 2 :</p> <p>Données : commencent à finissent à</p> <p>↙ ↘</p> <p>Paquet 1 (données)</p> <p>Hardware type :</p> <p>Protocole :</p> <p>Longueur @MAC :</p> <p>Longueur @IP :</p> <p>Operation :</p> <p>@MAC Source :</p> <p>IP Source :</p> <p>MAC Destination :</p> <p>IP Destination :</p>	<p>@MAC Destination:</p> <p>@MAC Source :</p> <p>Protocole couche 2 :</p> <p>Données : commencent à finissent à</p> <p>↙ ↘</p> <p>Paquet 2 (données)</p> <p>Hardware type :</p> <p>Protocole :</p> <p>Longueur @MAC :</p> <p>Longueur @IP :</p> <p>Operation :</p> <p>@MAC Source :</p> <p>IP Source :</p> <p>MAC Destination :</p> <p>IP Destination :</p>

A quoi servent les 18 octets restants en fin de trame ?

Conclusion : A quoi a servi cet échange de trames ?