R&T1 R2 TD5
Annexe : Trames et protocoles

Présentation

L'encapsulation des données du modèle OSI peut se représenter (pour quelques exemples de protocoles) de la manière suivante :

Format données	***Protocoles***	***Niveau OSI***
messages	**FTP, DNS, Bootp,...**	5, 6 et 7
	⇩	
segments	**ICMP, TCP, UDP**	4
	⇩	
paquets	**IP, ARP, RARP**	3
	⇩	
trames	**Ethernet, 802.11, LLC ...**	1 et 2

La **taille** des champs est, par défaut, comptée en **nombre d'octets**.

1. Niveau Trame

1.1 Protocole Ethernet

Préambule	**Destination**	**Source**	**Type**	**Données couches supérieures**	**CRC**
8	6	6	2	46-1500	4

Liste de quelques **types** de trame ethernet :

0x0800	Internet Protocol (**IP**)
0x0806	Address Resolution Protocol (**ARP**)
0x8035	Reverse Address Resolution Protocol (**RARP**)

1.2 Protocole 802.11

Il y a trois principaux types de trames (données, contrôle et gestion), nous ne retiendrons ici que les trames de données. Les trames à destination d'un point d'accès (AP) peuvent être retransmis dans la cellule (BSS) ou vers le filaire (DS)

Contrôle de trame	Durée / ID	Adr. 1	Adr. 2	Adr. 3	Contrôle de séquence	Adr. 4	Données couches supérieures	CRC
2	2	6	6	6	2	6	0-2312	4

Remarque : les champs ne sont pas tous utilisés. Cela dépend du contexte.

Contrôle de trame : version, type de trame, sous-type... (ces deux octets se lisent dans l'ordre poids faible puis poids fort, l'interprétation des bits se fait du poids faible vers le poids fort).

Dans ce champ se trouve le bit ToDS (pour le système de distribution) et from DS (vient du filaire) dont la valeur définit le nombre d'adresses dans la trame.

Liste de quelques types **contrôle de trame**:

0x0208	**Données** de DS vers STA via AP
0x0A08	**Données retransmises** de DS vers STA via AP

Durée / ID : temps (en microsecondes) pendant lequel le canal sera alloué ou **Id**entifiant de connexion.

Adresse 1 : est toujours l'adresse du récepteur (ie. la station de la cellule qui est le récepteur support du paquet). Si ToDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station.

Adresse 2 : est toujours l'adresse de l'émetteur (ie. celui qui, physiquement, transmet le paquet). Si FromDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station émettrice.

Adresse 3 : est l'adresse de l'émetteur original quand le champ FromDS est à 1. Sinon, et si ToDS est à 1, Adresse 3 est l'adresse destination.

Adresse 4 : est utilisé dans un cas spécial, quand le système de distribution sans fil (Wireless Distribution System) est utilisé et qu'une trame est transmise d'un Point d'Accès à un autre. Dans ce cas, ToDS et FromDS sont tous les deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire. Nous considérerons que ce champ n'existe pas.

contrôle de séquence : non étudié (pour la fragmentation)

Données couches supérieures : les premières données correspondent à la trame LLC (802.2)

1.3 Protocole 802.2

Offre 3 types de services : LLC1 (sans connexion ni acquittement), LLC2 (avec connexion et acquittement) et LLC3 (sans connexion avec acquittement).

On se limitera au format de la trame LLC1

DSAP	SSAP	Contrôle	Organization	Type	Données couches supérieures
1	1	6	3	2	N

DSSAP : Adresse destinataire (0xaa)
SSAP : Adresse source (0xaa)
Contrôle : 0x03 = UI (Information non numérotée)
0xFF = XID (Echange d'identificateur)
0xF3 = TEST
Organization : 0x000000 = Encapsulé dans Ethernet
Type : type de paquet de la zone des données voir (1.1)

2. Niveau Paquet

2.1 Protocole ARP ou RARP

La protocole ARP permet de récupérer l'adresse MAC à partir d'une adresse IP, le protocole RARP de récupérer l'adresse IP connaissant l'adresse MAC.

Type de réseau de niveau 2	**Type de protocole de niveau 3**	**Long. Adresse niveau 2**	**Long. Adresse niveau 3**	**Type d'opération (code ARP)**
Adresse Ethernet de l'émetteur				**Adresse IP de l'émetteur...**
... Adresse IP de l'émetteur	**Adresse Ethernet du récepteur**			
Adresse IP du récepteur				
2	2	1	1	2

Liste de quelques **types de réseau de niveau 2** :

0x0001	**Ethernet**

Liste de quelques **types de protocole de niveau 3** :

0x0800	Internet Protocol (**IP**)

Long. Adresse niveau 2 et Long. Adresse niveau 3 en octets

Liste des différents **types d'opération** :

0x0001	Requête **ARP**
0x0002	Réponse **ARP**
0x0003	Requête **RARP**
0x0004	Réponse **RARP**

2.2 Protocole IP (ou datagramme)

Version	**Long. entête**	**Service**	**Long. totale**	
Numéro paquet			**Flags**	**Numéro fragment**
bits 31-28	bits 27-24	bits 23-16	bits 15-13	bits 12-0
Time To Live		**Type Protocole de niveau 4**	**CRC**	
Adresse IP de l'émetteur				
Adresse IP du récepteur				
Options				**Bourrage**
Zone de données couche 4				
variable				variable

Version : 0x04 pour IPV4

Long. entête : en nombre de mots de 32 bits depuis le champs **Version** jusqu'au champs **Adresse IP du récepteur** inclus.

Service : non étudié (0x00 signifie TOS normal).

Long. totale : longueur totale du datagramme IP en octets depuis le champs Version jusqu'au dernier octet de la **Zone de données couche 4**.

Numéro paquet : numéro d'identification du paquet.

Flags : non étudié (pour la fragmentation)

Numéro fragment : non étudié (pour la fragmentation)

Time to Live : représente le temps pendant lequel le datagramme peut circuler sur le réseau. Cette valeur est décrémentée après chaque passage dans un routeur, la trame est détruite quand cette valeur passe à 0.

Type Protocole de niveau 4 : voir ci-dessous

Options et Bourrage : doivent toujours constituer un multiple de 32 bits.

Liste de quelques **types Protocole de niveau 4** :

0x01	**ICMP**
0x06	**TCP**
0x11	**UDP**

3. Niveau segment

3.1 Protocole ICMP

Précédée d'une trame IP, permet de transmettre des messages d'erreurs divers. Le champs de données est de taille variable.

Type de Message	**Code**	**Cheksum**
1	1	2
Données ICMP		

Liste de quelques **types de Message** :

0x00	**Echo** réponse
0x08	**Echo** requête

Liste de quelque(s) **Code(s)** :

0x00	Pour des Messages de type **Echo** (ping par ex.)

3.2 Protocole TCP

Ce protocole est identifié par la valeur 6 dans le champ **types Protocole de niveau 4** du paquet IP.

Port source								Port destination
Numéro de séquence								
Numéro d'acquittement								
Long. entête	Réservé	URG	ACK	EOM	RST	SYN	FIN	Fenêtre
Cheksum								Priorité
bits 31-28		bits 21-16						bits 15-0
Options								Bourrage
Zone de données couche 5 et plus								
variable								variable

Liste de quelques numéros de **Port** :

N° de port	7	20	21	22	25	37	67	68	80	110	161
Service	**Echo**	**FTP données**	**FTP contrôle**	**SSH**	**SMTP**	**Time**	**Bootps**	**Bootpc**	**HTTP**	**POP3**	**SNMP**

(Les valeurs supérieures à 1024 correspondent à des ports clients)

Numéro de séquence : numéro du premier octet transmis dans le segment

Numéro d'acquittement : numéro de séquence du prochain octet attendu par l'émetteur.

Long. entête : en nombre de mots de 32 bits depuis le champs **Port source** jusqu'au champs **Bourrage** inclus.

URG ... FIN : non étudié (6 bits de contrôles divers)

Fenêtre : nombre d'octets que le récepteur peut accepter à partir du numéro d'acquittement.

Cheksum : sans commentaire !

Priorité : contient un pointeur sur les octets traités en priorité si le bit **URG**=1

Options et Bourrage : doivent toujours constituer un multiple de 32 bits.

3.3 Protocole UDP

Ce protocole est identifié par la valeur 0x11 dans le champ **types Protocole de niveau 4** du paquet IP.

Port source	Port destination
Longueur	Cheksum
Zone de données couche 5 et plus	
2	2

Liste de quelques numéros **Port** : voir format message TCP

Longueur : en octets depuis le champs **Port source** jusqu'au champs **Zone de données couche 5 et plus** inclus.

Cheksum : sans commentaire !

4 Niveau message

4.1 BOOTP

Ce protocole est encapsulé dans un message UDP.

Op	**htype**	**hlen**	**hops**	**xid**			
xid				**secs**		**bootp flag**	
ciaddr				**yiaddr**			
siaddr				**giaddr**			
chaddr						**sname...**	
... sname (64 octets)							
filename...							
...filename (128 octets)							
vend (64 octets)							
1	1	1	1	1	1	1	1

Op : Type de message/code **op**ératoire du paquet
0x01 = BOOTREQUEST (requête d'amorçage)
0x02 = BOOTREPLY (réponse d'amorçage)

htype : Type d'adresse matérielle
0x01 = Ethernet

hlen : Longueur de l'adresse matérielle
(p.ex. 6 pour ethernet 10 Mbps).

hops : Fixé par le client à zéro ; peut être utilisé par des passerelles lors de d'amorçages au travers de passerelles.

xid : ID de transaction : nombre aléatoire utilisé pour associer cette requête de démarrage avec la réponse qu'elle génère.

secs : Rempli par le client, secondes écoulées depuis le début de sa tentative d'amorçage. (inutilisé)

bootp flag : non étudié

ciaddr : Adresse IP du client ; remplie par le client dans la requête d'amorçage si elle est connue.

yiaddr : « Votre » adresse IP (client) ; remplie par le serveur si le client ne connaît pas sa propre adresse (si ciaddr valait 0).

siaddr : Adresse IP du serveur renvoyée dans réponse d'amorçage par le serveur.

giaddr : Adresse IP de la passerelle utilisée dans l'amorçage au travers de passerelles optionnel.

chaddr : Adresse matérielle (MAC) du client ; remplie par le client.

sname : Nom de l'hôte serveur, chaîne de caractères terminée par un caractère NUL.

filename : Nom du fichier de démarrage, chaîne de caractères terminée par un caractère NUL ; nom « générique » ou null dans la requête d'amorçage, nom de chemin de répertoire complètement qualifié dans la réponse d'amorçage.

vend : zone optionnelle spécifique au vendeur pourrait p.ex. être le type/numéro de série du matériel dans la requête, ou une « capacité » du système de fichiers distant lors de la réponse. Champ complété par du bourrage.

Magic (4 octets) : non étudié

options (taille dépend de l'option) : 1 octet **numéro de l'option**, **nombre d'octets** associés à l'option, n octets selon l'option :

Num. option (décimal)	**Nombre d'octets**	**Signification**
1	4	Masque de sous-réseau
3	4	Adresse IP de la passerelle
6	8	Adresses (2) IP des DNS
15	variable	Nom de domaine
50		
51	4	Durée du bail (en seconde ?)
53	1	Message DHCP : 3 = DHCP Request 5 = DHCP ACK
54	4	Adresse IP du serveur DHCP
55	7 (par. ex)	Liste des paramètres demandés lors d'une requête
255	0	Fin des options

4.2 DNS

Ce protocole utilise le même format de message pour les demandes et les réponses.

Identificateur	**Flags**
Nombre de questions	**Nombre de réponses**
Nombre d'enregistrements « autorité »	**Nombre d'enregistrements « informations suplémentaires »**
Questions (n octets)	
Réponses (n octets)	
Autorité (n octets)	
Informations supplémentaires (n octets)	
2	2

Identificateurs : une valeur permettant de faire corespondre demande et réponse.

Flags : indications sur le message
0X0100 = requête standard
0x8181 = réponse à une requête => pas d'erreur
0x8583 = réponse à une requête => pas trouvé le nom