Les Réseaux

les protocoles TCP/IP

Version 3
Auteur : Christophe VARDON
professeur STI – Bac Pro MRIM
formateur TICE iufm

Table des matières

1. Historique - Applications

Ce protocole de communication a été mis au point à partir d'une étude commandée au début des années 1970 par le DARPA (Defense Advanced Project Research Agency) dépendant du DoD (Department of Defense) Américain. L'objectif était de mettre au point un protocole de communication permettant d'interconnecter les ordinateurs de toutes marques dont disposait l'armée des US.

Les premières implémentations ont été réalisées au début des années 1980 . Elles introduisaient les notions de : couches de communication. Le protocole TCP/IP ne respecte pas totalement la norme OSI.

1.1. Les atouts TCP/IP

Il a été « adopté » très tôt par les systèmes Unix, ce qui lui apporté fiabilité et crédit. Les spécifications sont du domaine public, et elles sont facilement accessibles à tous, ce qui a permis de nombreux développements dans les milieux universitaires et de la recherche. Les spécifications sont fournies sous la forme de RFC (Request for Comments).

Diversité technologique : il est disponible sur la plupart des plates-formes matérielles et systèmes d'exploitation, de l'ordinateur personnel (PC ou Mac) au plus gros calculateur vectoriel (Cray, ...).
Adaptabilité technique : Il est utilisable sur la plupart des réseaux physiques (Ethernet 802.3 , Token Ring 802.5, liaisons séries) et même à travers d'autres réseaux publics (X25, Numéris).
Diversité logicielle : De très nombreux logiciels ont été développés sur TCP/IP, qu'ils soient du domaine public ou vendus par des sociétés spécialisées.

C'est le principe de : ***IP au-dessus de tout ,*** il fonctionne sur :	
Ethernet (RFC894) Token Ring Liaison série de 9,6Kbits/s à 2Mbits/s SLIP (RFC1055) PPP (Point to Point Protocol), X25	FDDI (RFC1188) FastEthernet 100Mbps ATM

1.2. Quelles applications ?

- r-commands : (ou remote commandes) : exécution d'une commande à distance sur une autre machine du réseau local
- telnet : connexion interactive
- ftp (File Transfert Protocol) : transfert de fichier
- smtp (Simple Mail Tranfert Protocol) : messagerie
- nfs : (Network File System): système de fichiers répartis

Sur un même réseau physique (Ethernet par exemple) le protocole TCP/IP peut cohabiter avec d'autres protocoles de niveau 3 . Pour cela dans la trame de niveau 2 un champ identifie le type de protocole de niveau 3.

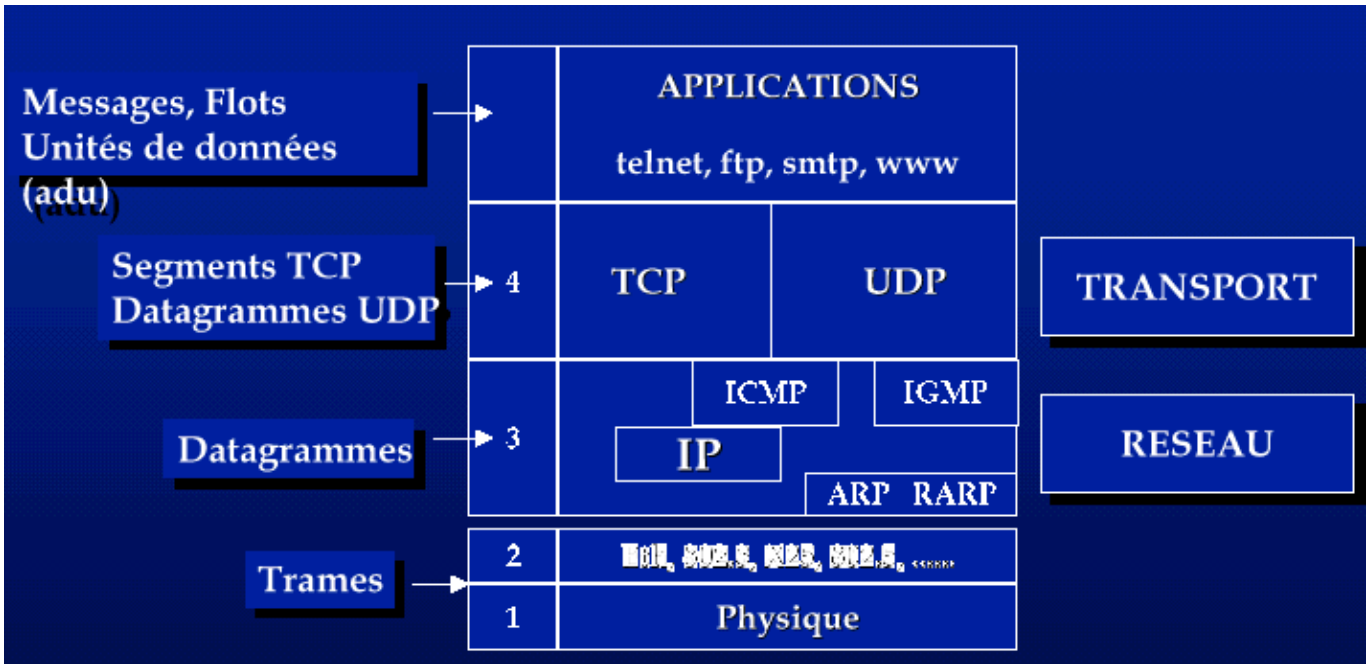
1.3. Protocole, pilote, interface

Plusieurs protocoles peuvent même cohabiter sur une même machine : le niveau 2 est géré par le pilote (driver) de la carte (Ethernet par ex), au dessus duquel il y a plusieurs "piles" de niveau supérieur. Le paquet extrait de la trame est transmis à la pile correspondant au type de protocole (cf notion de SAP - Service Access Point - du modèle OSI)

1.4. Version de IP

On utilise actuellement la version 4 de TCP/IP (dite : ipv4), et on passera progressivement à la version 6 (dite : ipv6)dans les années à venir .

1.5. Place dans le modèle OSI



2. A quoi servent les protocoles TCP/IP ? : fonctionnalités des protocoles IP, TCP, ARP, ICMP

***PROBLÈME* :** comment identifier la machine destinataire d'un message circulant sur le réseau ?
***(MAUVAISE) RÉPONSE* :** l' « adresse » MAC de la carte réseau n'est pas suffisante car elle ne donne aucune indication sur le réseau dont fait partie la machine : on est limité au réseau local;
***(BONNE) RÉPONSE* :** Il faut une adresse qui identifie la machine elle-même, mais aussi le réseau (LAN) dont elle fait partie.

➔ le protocole IP autorise l'attribution d'une adresse de type ***réseau.machine*** à chaque poste informatique.

➔ l'adresse IP permet d'identifier le réseau et la machine destinataire d'un message.

➔ Conclusion : le protocole IP a pour rôle d'identifier la source et le destinataire d'une trame et de fournir une route pour son acheminement. (fonction de routage)

Oui, mais : sur la machine destinataire peuvent tourner plusieurs logiciels; par exemple « *Internet Explorer* » pour naviguer sur le Web et « *Outlook Express* » pour le courrier électronique.

➔ ***PROBLÈME :*** comment le système d'exploitation va-t-il savoir à quelle application sont destinées les données recues ?
➔ ***RÉPONSE :*** le protocole TCP rajoute à la trame un numéro (appelé « port TCP ») qui indique l' application destinataire des données (ex : le port 80 pour le web/http)

➔ **Un socket** est une adresse réseau constituée par la concaténation d'une adresse Internet avec un numéro de port TCP (ex : **192.168.1.2:80**).

« Well known ports »

Les numéros de port standarts sont définis la **RFC1700**; complétez le tableau suivant :

Application	*n° du port TCP*	*Application*	*n° du port TCP*
Web - http (ex : IE5.5)		Transfert de fichier - ftp	
Mail - smtp (ex : Outlook)		courrier entrant - pop	
proxy http (ex : squid proxy serv)		partage de fichier - netbios	
administration distante - snmp			
telnet (remote terminal)			

3. Analyse du protocole IP (Internet Protocol)

L'adresse IP d'une machine est une adresse de niveau réseau codée sur 32 bits (ie 4 octets en IPv4) qui est en général notée sous la forme de 4 chiffres séparés par des points. On parle de notation en décimal pointé. Chaque champ, qui représente un octet, peut prendre des valeurs entre 0 et 255.

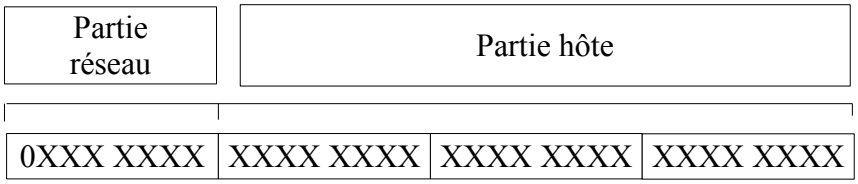
Exemple : *192.93.116.3*

3.1. Structure d'une adresse IP

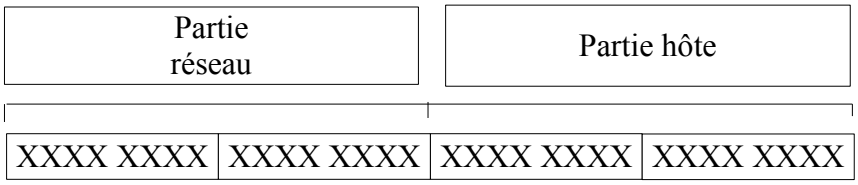
L'adresse IP est constituée d'un champ *numéro de réseau* (1, 2 ou 3 octets) et d'un champ *numéro de machine dans le réseau* (3, 2 ou 1 octets). L'adresse ip = adresse de réseau + adresse de machine.

Les réseaux TCP/IP sont rangés en 3 classes A, B ou C :

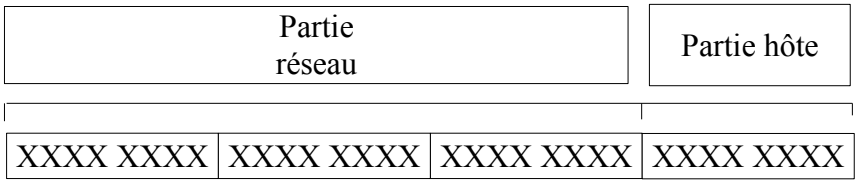
- classe A : 1 à 127 .X.X.X



- classe B : 128 à 191 .X.X.X



- classe C : 192 à 223 .X.X.X (les adresses > à 223 sont réservées à d'autres usages)



Le nombre de machines dans le réseau dépend donc de la classe du réseau. Chaque octet du champ machine peut prendre des valeurs entre 1 et 254. Les valeurs 0 (tous les bits à 0) et 255 (tous les bits à 1) sont réservées :

- Un champ machine tout à 0 sert à désigner le numéro de réseau (notamment pour le routage)

- Un champ tout à 1 indique un message de broadcast adressé à toutes les machines IP du réseau.

3.3. Des adresses réservées!

- **0.0.0.0** est réservée pour la route par défaut. L'adresse désigne tous les réseaux. Tous les paquets destinés à un réseau inconnu, seront dirigés vers cette route.
- **127.0.0.0** est réservée au trafic IP de la machine locale. Une interface locale porte en générale l'adresse 127.0.0.1 appelée adresse de "loopback" ou boucle locale.
- Trois plages d'adresses peuvent être librement utilisées pour monter un réseau privé. Voici ces adresses : Classe A **10.x.x.x**, Classe B **172.16.x.x à 172.31.x.x**, Classe C **192.168.x.x**.

Note : aucun paquet provenant d'un réseau privé ou à destination d'un réseau privé, ne peut (ou ne doit...) être routé sur l'internet.

3.4. Les domaines et les noms de machine

- Il est peu commode de désigner une machine par son adresse IP.

➔ L'utilisateur « humain » utilise un nom qui se présente sous la forme : *nom_machine.sous_domaine.domaine* (ex : www.google.fr).

- Malgré tout, c'est l'adresse IP chiffrée qui est utilisée en interne dans les paquets au cours des échanges. Il faut donc un mécanisme qui permette de traduire le nom_machine en adresse IP.

➔ Des ordinateurs appelés « Serveurs de noms » ou « DNS » se chargent de cette traduction

3.5. La fonction de routage

Les réseaux IP sont interconnectés par des « routeurs » IP (parfois appelés « passerelles »). Chaque station IP doit connaître le routeur par lequel il faut sortir pour pouvoir atteindre un réseau extérieur.

Un routeur dispose de plusieurs interfaces réseau et contient une table qui lui indique sur quelle interface tel ou tel réseau est relié. Il oriente donc **physiquement** la trame sur la bonne **route**!

Exemple :

- Réseau 1 --> Interface Ethernet 1
- Réseau 2 --> Interface Ethernet 2
- Autres réseau --> Interface Modem

Les tables de routage peuvent être statiques dans le cas de réseaux simples, ou dynamiques dans le cas de réseaux maillés. Le protocole d'échange dynamique des tables IP sur un réseau local est *RIP* (Routing Information Protocol) ou le protocole OSPF.

3.6. Les masques de (sous-)réseau

Les masques de réseau

Pour que le réseau Internet puisse router (acheminer) les paquets de données, il faut qu'il connaisse l'adresse IP du réseau local de destination. Pour la calculer à partir de l'adresse IP de destination, on utilise le masque de sous réseau.

A chaque classe d'adresses est associé un masque de réseau, ou netmask, qui est constitué de 32 bits. Le tableau suivant fournit les différents masques pour les trois classes traditionnelles.

Classe	Masque
A	255. 0. 0. 0
B	255. 255. 0. 0
C	255. 255. 255. 0

Un « ET » logique appliqué entre le masque de réseau et l'adresse IP permet d'obtenir l'adresse d'un réseau correspondant.

Calcul de l'adresse réseau en décimal

@ IP	193	252	19	3
Masque Réseau	255	255	255	0
@ Réseau	193	252	19	0

Calcul de l'adresse réseau en binaire

@ IP	1100 0001	1111 1100	0001 0011	0000 0011
Masque Réseau	1111 1111	1111 1111	1111 1111	0000 0000
@ Réseau	1100 0001	1111 1100	0001 0011	0000 0000

Ainsi, à l'aide du masque de réseau, on peut définir, pour toute adresse IP :

L'adresse réseau associée, la partie hôte associée, l'adresse de diffusion associée qui désigne tous les hôtes de ce réseau.

Le tableau suivant fournit ces informations pour trois adresses IP prises parmi les trois classes fondamentales.

Adresse IP	10. 25. 2. 5	172. 17. 5. 8	192. 168. 53. 24
Classe	A	B	C
Masque de réseau	255. 0. 0. 0	255. 255. 0. 0	255. 255. 255. 0
Adresse de réseau	10. 0. 0. 0	172. 17. 0. 0	192. 168. 53. 0
Adresse de diffusion	10. 255. 255. 255	172. 17. 255. 255	192. 168. 53. 255
Complément à 1 du masque	0.255.255.255	0.0.255.255	0.0.0.255
Partie hôte de l'adresse	0.25.2.5	0.0.5.8	0.0.0.24

Les masques de sous - réseaux

Parfois, on est amené à répartir les adresses IP d'un même réseau de classe A, B ou C sur plusieurs supports physiques. Par exemple , si on dispose d'une cinquantaine de machines, à répartir sur trois réseaux Ethernet par exemple, il serait inutilement couteux d'acheter trois réseaux de classe C : une seule classe C peut déjà accueillir 254 machines.

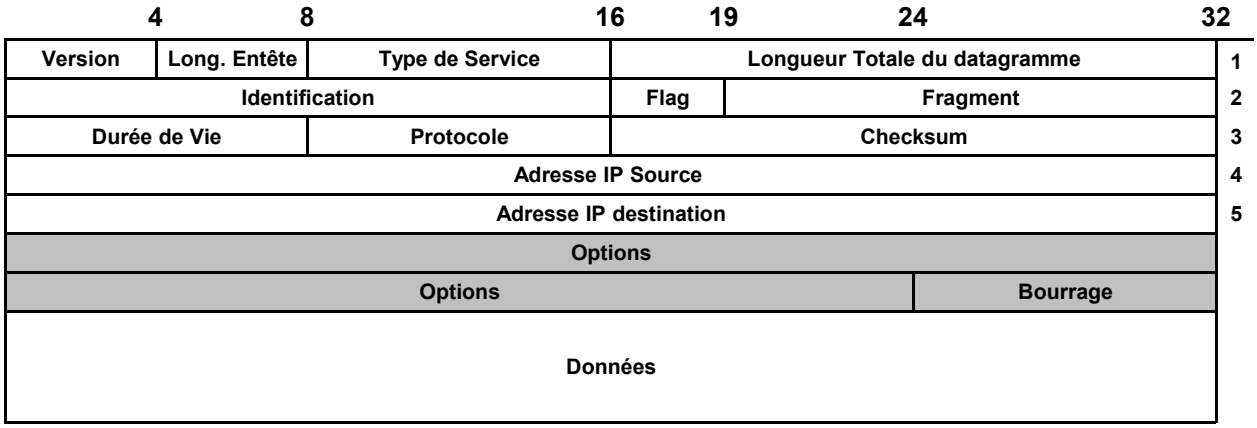
➔ Pour résoudre ce problème, il faut introduire un nouveau type de masque : le masque de sous - réseaux.

Le principe est simple : le réseau est découpé en sous - réseaux de même taille. Pour cela, **la partie hôte des adresses est elle-même découpée en deux plages de bits** :

la plage des bit de poids forts correspond aux bits identifiant les sous réseaux
l'autre plage désigne le numéro de machine dans le sous réseau.

3.7 Description du datagramme IP :

La structure générale d'un datagramme IP est représentée sur la figure suivante :



Version (Vers)
Sur ces 4 bits est codé le numéro de version du protocole IP utilisé. Actuellement, il s'agit pratiquement toujours de la version **4 (0100)**. Le numéro **5** sert à des applications expérimentales et la version **6** est en cours de mise en service (celle-ci utilise une autre structure de datagramme).

Longueur d'entête (I.H.L.)
Comme la longueur d'une entête de datagramme IP est variable, elle est codée sur 4 bits, sous forme de mots de 32 bits (4 octets). (Par exemple, **5** représente 5 fois 32 bits, soit **20 octets**).

Type de service (Type of Service ToS)
Ce champ de *8 bits* possède la structure suivante : *(Pour l'instant une seule option peut être sélectionnée)*

Priorité			Type de Service				
			-délai	+débit	+fiable	-coût	0
0	1	2	3	4	5	6	7

- 3 bits indiquant la priorité.
  - 000 (Par défaut - priorité la moins élevée)
  - 111 (supervision réseau- priorité la plus élevée). Cette partie est utilisée par certaines passerelles.

- 4 bits indiquant le type de service souhaité (en fonctionnement normal, ils sont tous à zéro) :
  - Le premier bit demande au routeur de choisir un chemin ayant un délai de transmission le plus court possible (par exemple choisir de passer par un câble sous marin plutôt que par une liaison satellite)
  - Le deuxième bit demande au routeur un débit élevé.
  - Le troisième bit demande au routeur de diriger les paquets vers des liaisons fiables
  - Le quatrième bit demande au routeur de choisir un chemin ayant un coût minimum.

- 1 bit réservé pour le futur, devant actuellement rester à zéro sauf pour certains cas expérimentaux.

Longueur du datagramme (Long. Totale)
Longueur totale du datagramme (entête + données), en octets. Comme ce champ est codé sur 16 bits, la longueur maximale d'un datagramme IP est de 65535 octets. **Attention :** si un datagramme est fragmenté, ce champ fait référence à la longueur du fragment courant et non à la longueur du datagramme initial.

Fragmentation
Si le routeur reçoit un datagramme trop grand pour le support sur lequel il doit l'envoyer, il est obliger de fragmenter ce datagramme. Il est donc nécessaire de repérer ces fragments et de faire en sorte que le récepteur des fragments d'un datagramme puisse « recoller » les morceaux dans le bon ordre pour reconstituer le datagramme. 3 champs permettent de résoudre ce problème.

Identification (ID)
Ce champ sur 16 bits sert à identifier un datagramme ou les fragments d'un datagramme fragmenté. En effet, ce champ a *la même valeur pour tous les fragments provenant d'un même datagramme*.

Drapeau (Flg)
Ces 3 bits donnent des informations concernant la fragmentation :

0	DF	MF

- ✔ Le premier n'est pas utilisé et doit rester à zéro.
- ✔ Le deuxième sert à *interdire la fragmentation* du datagramme (0 - Autorisé, 1 - Interdit) (appelé bit de « non-fragmentation » ou « Don't Fragment » DF).
- ✔ Le troisième est à zéro s'il s'agit du *dernier fragment* du datagramme et à un si d'autres fragments doivent encore arriver (appelé bit « fragments à suivre » ou « More Fragment » MF).

Place du fragment (Fragment)
Ce nombre codé sur 13 bits indique la position qu'a le 1er octet de donnée du fragment dans le datagramme (non fragmenté). **Ce nombre est un multiple de 8 octets**. Ainsi, une valeur de 10 signifierait que le 1er octet de donnée de ce fragment est en fait l'octet 80 du datagramme non fragmenté. S'il s'agit du premier fragment, ou si le datagramme n'est pas fragmenté, tous les bits sont à zéro.

Durée de vie (Time to Live TTL)
Théoriquement, ce champ doit indiquer sur 8 bits le nombre de secondes pendant lequel le datagramme est autorisé à voyager. A chaque passage d'une passerelle, on retire le temps qu'a pris la traversée de la passerelle. En pratique, comme ce temps est souvent inférieur à une seconde, on retire 1, ce qui fait que ce champ indique plus souvent le nombre de passerelles par lesquelles le datagramme peut passer qu'une durée proprement dite. Quand le champ durée de vie atteint zéro, le datagramme est détruit et un message d'erreur est envoyé à l'émetteur. Cette méthode permet d'éviter qu'un datagramme ne circule indéfiniment en boucle.

Numéro de protocole (Protocole)
Ce champ de 8 bits indique à quel protocole de niveau plus élevé est destiné le datagramme (SAP). La valeur zéro est réservée. Quelques exemples de valeurs : (La liste complète se trouve dans la RFC 790)

1 : ICMP (Internet Control Message Protocol)
6 : TCP (Transmission Control Protocol)
17 : UDP (User Datagram Protocol)

Adresse IP source
Adresse IP de l'émetteur du datagramme.

Adresse IP destination
Adresse IP du destinataire du datagramme.

Données
Ce sont les données du datagramme proprement dites.

Résumé :
Le protocole Internet est responsable de **l'adressage** et du **routage** entre machines, du cheminement des paquets de données dans le réseau, de la constitution et du réassemblage des paquets. Les fonctionnalités assurées par IP peuvent se déduire de l'examen de l'en-tête du paquet. Il identifie entre autres la source et la destination du paquet et comporte des identificateurs de fragmentation.

4. Analyse des protocoles TCP et UDP (Transfert Control Protocol)

Nous avons jusqu'à présent surtout parlé de la partie « **IP** »; nous allons maintenant étudier la partie « **TCP** » de TCP/IP.

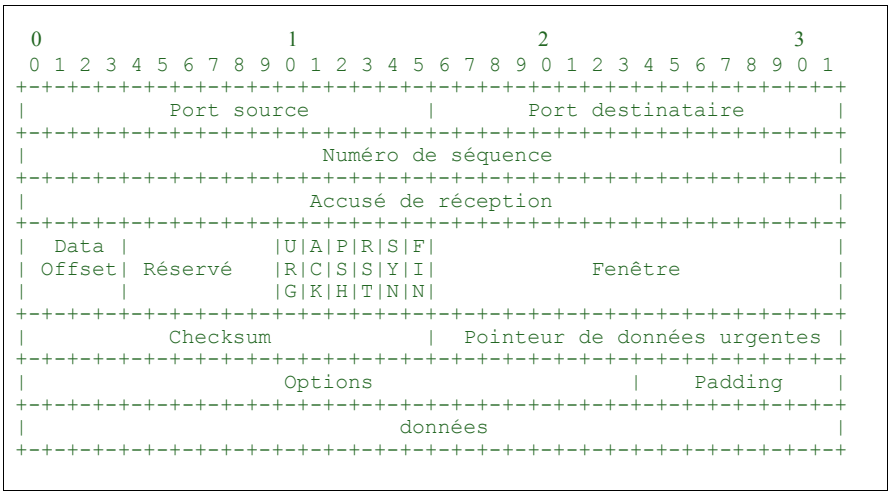
Extrait de la RFC793 : « TCP fournit un moyen d'établir une communication fiable *entre deux tâches* exécutées sur deux ordinateurs autonomes raccordés à un réseau de données. »

4.1. Fonctionnalités

Le protocole TCP est le protocole majeur de toute l'architecture INTERNET. C'est un protocole qui fonctionne en **mode connecté**. Il dispose d'un ensemble de fonctionnalités. En voici quelques unes :

- Identification précise de l'émetteur et du destinataire
- Gestion des accusés de réception
- Délivrance de données fiable, séquentielle et sans duplication
- Mécanisme de contrôle de flux
- Connexions passives et actives
- Multiplexage (plusieurs connexions simultanées sur un même support).

4.2. Description du segment



Port source: 16 bits
Le numéro de port de la source.

Port Destinataire: 16 bits
Le numéro de port du destinataire.

Numéro de séquence: 32 bits
Le numéro du premier octet de données par rapport au début de la transmission (sauf si SYN est marqué). Si SYN est marqué, le numéro de séquence est le numéro de séquence initial (ISN) et le premier octet à pour numéro ISN+1.

Accusé de réception: 32 bits
Si ACK est marqué ce champ contient le numéro de séquence du prochain octet que le récepteur s'attend à recevoir. Une fois la connexion établie, ce champ est toujours renseigné.

Data Offset: 4 bits
La taille de l'en-tête TCP en nombre de mots de 32 bits. Il indique là ou commence les données. L'en-tête TCP, dans tous les cas à une taille correspondant à un nombre entier de mots de 32 bits.

Réservé: 6 bits

Réservés pour usage futur. Doivent nécessairement être à 0.

Bits de contrôle: 6 bits (de gauche à droite):

- URG: Pointeur de données urgentes significatif
- ACK: Accusé de réception significatif
- PSH: Fonction Push
- RST: Réinitialisation de la connexion
- SYN: Synchronisation des numéros de séquence
- FIN: Fin de transmission

Fenêtre: 16 bits

Le nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir.

Checksum: 16 bits

La somme de contrôle

Pointeur de données urgentes: 16 bits
Communique la position d'une donnée urgente en donnant son décalage par rapport au numéro de séquence. Le pointeur doit pointer sur l'octet suivant la donnée urgente. Ce champs n'est interprété que lorsque URG est marqué.

Options: variable

Les champs d'option peuvent occuper un espace de taille variable à la fin de l'en-tête TCP. Ils formeront toujours un multiple de 8 bits. Un paramètre d'option commence toujours sur un nouvel octet.

Bourrage (padding): variable

Les octets de bourrage terminent l'en-tête TCP:

- de sorte que le nombre d'octet de celle-ci soit toujours multiple de 4 (32 bits)
- de sorte que l'offset de données marqué dans l'en-tête corresponde bien au début des données applicatives.

4.3. Etablissement d'une connection TCP

Considérons la capture de trame effectuée avec *Ethereal* :

```
No. Time        Source       Destination  Protocol Info
10 10.181832   192.168.0.10  212.27.35.1  TCP      4252 > http [SYN]
11 10.204707   212.27.35.1   192.168.0.10 TCP      http > 4252 [SYN, ACK]
12 10.204848   192.168.0.10  212.27.35.1  TCP      4252 > http [ACK]
13 10.205333   192.168.0.10  212.27.35.1  HTTP     GET / HTTP/1.1
```

L'établissement d'une connexion TCP suit un protocole strict :

- Une requête de synchronisation [**SYN**] de la part de l'initiateur du dialogue (le client),
- une réponse d'accusé réception de la synchronisation [**SYN,ACK**] de la part du serveur,
- un accusé réception du client [**ACK**]

4.4. Différences entre TCP et UDP

TCP est un protocole beaucoup plus complexe qu'UDP, il se charge, entre autres, de remettre en ordre, avant leur délivrance, les paquets qui lui parviennent.

Le protocole UDP (User Datagram Protocol) est un protocole de transmission de datagrammes sur le réseau qui fournit de manière optionnelle un certain nombre de contrôles. Un datagramme est un paquet de données considéré comme une entité isolée et indépendante, c'est-à-dire qu'il comporte dans son en-tête toutes les informations nécessaires à son acheminement à travers le réseau jusqu'à son destinataire.

La transmission de paquets composant le message est donc assurée de manière totalement indépendante pour chaque paquet. On pourrait, dans une certaine mesure, comparer ce type de service au service postal qui prend en charge les messages et assure leur transport à destination mais sans garantir le chemin parcouru par chaque message, ni le temps mis pour le parcourir, ni à fortiori le respect d'une séquentialité dans la délivrance des messages.

4.5. Etude de cas des services *WINDOWS XP Pro* et *2000 Advanced Server*

On utilise un outil de « hacker » pour lister les ports ouverts sur une machine *Windows* : cela nous permet de déterminer les services qui « tournent »; L'outil « **Nmap** » donne les résultant suivants sur un *Windows 2000 Advanced Server* :

```
Starting nmap V. 2.54BETA25 ( www.insecure.org/nmap/ )
Interesting ports on fenetre-w2k.hsc.fr (192.70.106.143):
(The 65524 ports scanned but not shown below are in state:
closed)
Port State Service
25/tcp open smtp
80/tcp open http
135/tcp open loc-srv
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1025/tcp open listen
1026/tcp open nterm
1027/tcp open unknown
3372/tcp open unknown
4983/tcp open unknown
Nmap run completed -- 1 IP address (1 host up) scanned in
115 seconds
```

```
nmap -sU 192.70.106.143 -p 1-65535
Starting nmap V. 2.54BETA25 ( www.insecure.org/nmap/ )
Interesting ports on fenetre-w2k.hsc.fr (192.70.106.143):
(The 65527 ports scanned but not shown below are in state:
closed)
Port State Service
135/udp open loc-srv
137/udp open netbios-ns
138/udp open netbios-dgm
445/udp open microsoft-ds
500/udp open isakmp
1028/udp open unknown
```

On fait de même avec une machine *XP Pro*; Finalement après avoir vérifié les applications correspondant à ces ports, voici les services ouverts en standard sous *2000* et *XP* :

Service	Port (s)	Service(s) Windows
Serveur IIS	25/tcp 80, 443/tcp 3456/udp >1024/tcp, >1024/udp	*SMTP (Simple Mail Transfert Protocol)* *Worid Wide Web Publishing Service* *IIS Admin Service* ? *2* ports dynamiques (RPC)
	<4000-5000>/tcp	1 port (site d'administration)
Protocole IKE	500/udp	*IPSEC Policy Agent*
NetBIOS sur TCP	137/udp, 138/udp, 139/tcp	*TCP/IP NetBIOS Helper Service*
CIFS/SMB	139/tcp, 445/tcp	*Server, Workstation*
Portrnapper RPC	135/tcp, 135/udp	*Remote Procédure Call (RPC)*
MSDTC	3372/tcp, >1024/tcp	*Distributed Transaction Coordinator*
Tâches programmées	>1024/tcp	*Task Scheduler*
Messenger	>1024/udp	*Messenger*

FIG. 1 - Services réseaux sur un système Windows 2000 serveur

Service	Port(s)	Service(s) Windows
Protocole IKE	500/udp	*IPSEC Policy Agent*
Protocole NTP	123/udp	*Windows Time*
UPnP	5000/tcp, 1900/udp	*SSDP Discover-y Service*
Cache DNS	>1024/udp	*DNS Client*
NetBIOS sur TCP	137/udp, 138/udp, 139/tcp	*TCP/IP NetBIOS Helper Service*
CIFS/SMB	139/tcp, 445/tcp	*Server, Workstation*
Portmapper RPC	135/tcp, 135/udp	*Remote Procédure Call (RPC)*
Tâches programmées	>1024/tcp	*Task Scheduler*
Messenger	>1024/udp	*Messenger*

FIG. 2 - Services réseaux sur un système Windows XP professionnel

5. Analyse du protocole ARP (Address Resolution Protocol)

C'est un protocole *de résolution (~traduction) d' adresse à l'intérieur du réseau local* (LAN)

L'adressage à l'intérieur d'un réseau local (~Ethernet!) se fait grâce à l'adresse MAC
> Ethernet ne connait pas les adresses IP! aïe ! > Il est nécessaire d'établir **un lien entre l'adresse IP d'une station et son adresse MAC** pour qu'un paquet IP arrivant dans un réseau local puisse être acheminé vers la bonne station. C'est le protocole ARP qui va permettre d'établir ce lien.

ARP traduit des adresses de type INTERNET sur 32 bits en adresses ETHERNET sur 48 bits. ARP se présente comme **un service** qui gère des **tables de correspondance d'adresses** et répond à des requêtes d'identification. Lorsqu'il reçoit une requête, il crée un **message de demande ARP : « qui possède l'adresse IP x.x.x.x ? »;** qui est diffusé (broadcast) à tout le réseau en attente d'une réponse positive de la part d'une des machines connectées. Une réponse positive provoque une mise à jour par ARP de ses tables de traduction d'adresses.

Par exemple : un équipement A veut envoyer un datagramme IP à un équipement B qui est connecté sur le même LAN; « Fatalement », il doit l'encapsuler dans une trame de la couche MAC (en général Ethernet-802.3). Le problème est que A ne connaît à priori que l'adresse IP de B et pas son adresse MAC. Il faut donc un protocole qui permette de découvrir l'adresse MAC de B à partir de son adresse IP. C'est le rôle du protocole ARP.

Voici quelques trames capturées avec Ethereal :

No.	Time	Source	Destination	Protocol	Info
1	0.000000	00:50:ba:eb:32:10	ff:ff:ff:ff:ff:ff	ARP	Who has 192.168.2.2? Tell 192.168.2.1
2	121353	00:40:f4:1c:d8:e4	00:50:ba:eb:32:10	ARP	192.168.2.2 is at 00:40:f4:1c:d8:e4
46	20.961	Micrsoft_54:00:00	Broadcast	ARP	Who has 213.36.80.1? Tell 213.36.24.90

➔ Commentez cette trames

➔ Capturez une demande et une réponse ARP avec Ethereal puis imprimez le détail de celle-ci. Commentez chaque ligne.

6. Analyse du protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) constitue le protocole des messages d'erreur. Les messages ICMP sont classés en plusieurs catégories :

La première est constituée de tous les messages résultant d'un incident réseau, où qu'il se soit produit, et qui peuvent être transmis à l'émetteur du paquet ayant subi l'incident. On peut classer dans cette catégorie les erreurs de routage ou celles qui résultent d'une indisponibilité du destinataire.

La seconde classe est constituée de tous les messages d'erreur induits par des incidents entre une machine hôte et la porte (gateway) par laquelle passent les paquets, par exemple, il peut s'agir d'une procédure de routage qui informe l'hôte d'un meilleur chemin que celui qui a été choisi à l'origine.

La dernière catégorie concerne tout ce qui est gestion de réseau, les tests de connexion, les mesures de performances et de trafic (ping).

Toutes les actions, transmissions ou redirections induites par un message ICMP sont prises en charge par la couche ICMP de IP.
Voici quelques trames capturées avec Ethereal lors d'une commande « ***ping 192.168.2.2*** »:

No.	Time	Source	Destination	Protocol	Info
5	0.233602	192.168.2.1	192.168.2.2	ICMP	Echo (ping) request
6	121353.49	192.168.2.2	192.168.2.1	ICMP	Echo (ping) reply

➔ Commentez cette trames

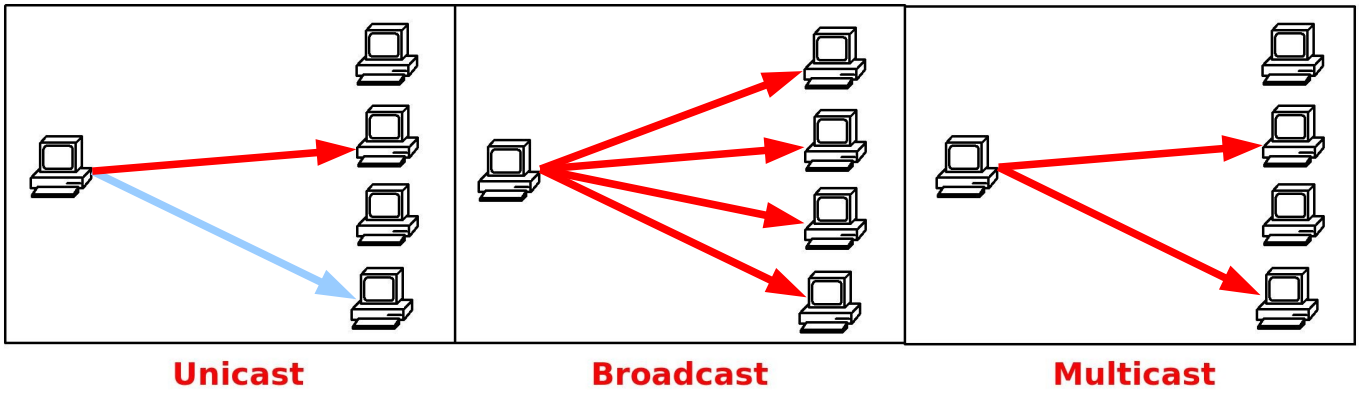
➔ Capturez une demande et une réponse ARP avec Ethereal puis imprimez le détail de celle-ci. Commentez chaque ligne.

7. La multidiffusion : le protocole IGMP

anglais	multicast	Modèle OSI	Niveau 3

Le protocole IGMP (**Internet Group Management Protocol**) est un protocole utilisé pour accéder à un groupe de multidiffusion IP.

La **multidiffusion** est une technique intégrée au protocole IP (multicast) qui permet à plusieurs machines destinataires de recevoir une même trame. Par rapport à du broadcast, qui s'adresse à toutes les machines du réseau, le muticast ne s'adresse qu'à un groupe de machines ciblées au sein du réseau.

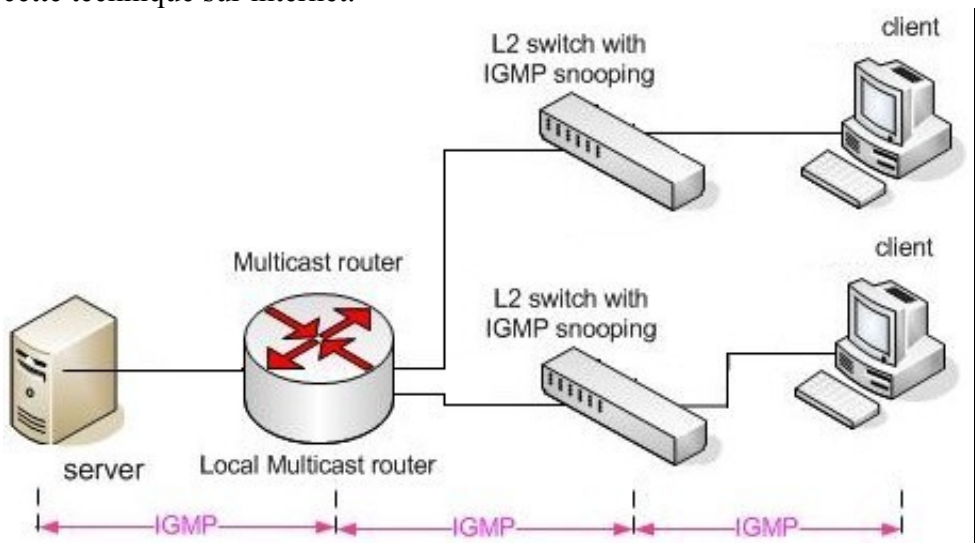


Le groupe d'ordinateur multicast est identifié par **une adresse IP de groupe multicast** de classe D. Le protocole IGMP permet à un PC de s'enregistrer dans ce groupe.

Rappel : la plage d'adresses de classe D va de **224.0.0.1** à **239.255.255.254**. Les adresses 224.0.0.1 à 224.0.0.255 sont réservés à des fonctions spécifiques au réseau local (LAN). Les adresses 239.0.0.0 – 239.255.255.255 sont réservées pour des usages privés.

7.2 Routage/commutation multicast

Pour que le mécanisme fonctionne, il faut qu'il existe dans le réseau un **routeur** qui gère le multicast et qui puisse se joindre au groupe multicast. Les switches qui gèrent le protocole IGMP peuvent remplir ce rôle. Par contre la plupart des routeurs internet ne le gèrent pas, ce qui explique qu'il est difficile d'utiliser cette technique sur internet.



Trafic généré :

1. le serveur envoie une seule trame au routeur multicast.
2. Le routeur envoie une trame vers chacun des 2 switches.
3. Chaque switch envoie une trame vers chacun des client qui font partie du groupe multicast.

7.3 IGMP Snooping

l' IGMP Snooping est la fonction intégrée dans certains commutateur, qui consistent à écouter et à gérer le trafic IGMP venant des clients et du serveurs.

Les commutateurs qui ne possèdent pas cette fonction transmettent les trames multicast sur tous leurs ports (e.g. en broadcast), ce qui génère un gros trafic inutile.

Dans le cas de l'IGMP snooping, le commutateur travaille **au niveau 3 du modèle OSI**; il doit conserver dans sa mémoire **une table pour chaque groupe multicast**; cette table contient les n° de port correspondants aux machines qui appartiennent au groupe. Quand il reçoit la trame multicast, il la retransmet sur tous ces ports.

Exemple :

La mise en fonction de l'IGMP snooping sur le Netgear FS726T est très simple.

Exemple 2 :

La mise en fonction de l'IGMP snooping sur le DLINK 1228 permet un réglage fin de nombreux paramètres.

Remarque : dans le cas de l'utilisation d'un concentrateur (HUB), il n'y a pas problème particulier puisque toutes les machines reçoivent toutes les trames : ce sont les cartes réseaux et le système d'exploitation du client qui gèrent l'IGMP.

7.4 Analyse d'un dialogue de multidiffusion impliquant IGMP

(source : http://www.reseaucerta.org)

Analyse et interprétation de la capture de trame lors d'une multidiffusion Ghost :

N°	Adresse Source	Adresse Destinataire	Protocole	Commentaire
1	Serveur	224.77.0.0	IGMP: Type 6, Ver2 Membership	Le serveur crée le groupe **224.77.0.0**
2	Client	224.77.0.0	UDP: D=6666 S=1025 LEN=268	Le client 'vérifie' l'existence du groupe **224.77.0.0**
3	Serveur	Client	UDP: D=1025 S=6666 LEN=268	Confirmation du serveur
4	Client	Serveur	TCP: D=1063 S=1025 - SYN	Connexion TCP en trois phases - Phase 1 - SYN
5	Serveur	Client	TCP: D=1025 S=1063 - SYN - ACK	Connexion TCP en trois phases - Phase 2 - SYN - ACK
6	Client	Serveur	TCP: D=1063 S=1025 - ACK	Connexion TCP en trois phases - Phase 3 - ACK
7 à 58	Client <--> Serveur		TCP protocole propriétaire Ghost	La connexion étant établie, le client et le serveur s'échangent divers paramètres ...comme le type de ghost (trame 10) **"clone,mode=pload,src=@mcdf"** le secteur de boot de la partition (trame 35)
59	Client	Serveur	TCP: D=1063 S=1025 - FIN	Le Client annonce la fin de la connexion
61	Serveur	Client	TCP: D=1025 S=1063 - FIN	Le Serveur annonce la fin de la connexion
63	Client	224.77.1.0	IGMP: Type 6, Ver2 Membership report	Le Client devient membre du groupe **224.77.1.0**
64	Client	Serveur	UDP: D=1061 S=7777	
65	Serveur	224.77.1.0	UDP: D=7777 S=1062	
66	Client	224.0.0.2	IGMP: Type 7, Leave Group	Le Client annonce au routeur qu'il quitte le groupe **224.77.1.0**
67	Client	224.77.3.44	IGMP: Type 6, Ver2 Membership	Le Client devient membre du groupe **224.77.3.44**
68 - 70	Client	Serveur	UDP: D=1061 S=7777	Échange d'informations dont le nom de la session : **@MCdf**
71	Serveur	224.77.3.44	UDP: D=7777 S=1062	
72	Serveur	224.0.0.2	IGMP: Type7, Leave Group	Le Serveur annonce au routeur qu'il quitte le groupe **224.77.0.0**
73	Serveur	224.77.3.44	UDP: D=7777 S=1062	
74 - 75	Client	Serveur	UDP: D=1061 S=7777	Le Serveur diffuse l'image. Le Client envoie des informations
76 - 81	Serveur	224.77.3.44	UDP: D=7777 S=1062	
82 - 87	Client	Serveur	UDP: D=1061 S=7777	
88 - 91	Serveur	224.77.3.44	UDP: D=7777 S=1062	
92 à 7921	Client --> Serveur Serveur --> 224.77.3.44		Succession de trames UDP	
7922	Client	224.0.0.2	IGMP: Type7, Leave Group	Le Client annonce au routeur qu'il quitte le groupe **224.7.33.44**

7.5 Le mappage des adresses IP multicast et MAC

Nous savons que l'adresse MAC correspondant à une adresse IP de Broadcast est **FF:FF:FF:FF:FF:FF**

Mais qu'en est-il quand nous sommes en présence d'adresses IP Multicast ? L'adresse IP (224.77.3.44) désigne un groupe destinataire, **il faut donc que l'adresse MAC associée désigne un groupe.**

Prenons la structure d'une adresse MAC classique :

00	-	A0	-	CC	-	E0	-	CF	-	D1
Zone OUI						**Zone Vendeur**				

La Zone OUI (Organizationally Unique Identifier) est un identifiant sur 3 octets attribué par IEEE.

L'octet de poids **fort** de la zone OUI possède une structure particulière.

N° du bit	7	6	5	4	3	2	1	0
signification							U/L	I/G

Si I/G = 0, il s'agit d'une adresse individuelle, si I/G = 1, il s'agit d'une adresse de groupe,
Si U/L = 0, il s'agit d'une attribution universelle, si U/L = 1, il s'agit d'une attribution locale.

Donc cela veut dire que pour une adresse MAC Multicast, **le bit de poids faible** de l'octet de poids fort sera égal à **1.** En réalité, une adresse MAC Multicast commence toujours par 01-00-5E-XX-XX-XX. Pour la partie Zone Vendeur, l'adresse Multicast est construite à partir de l'adresse IP. Les 23 bits de poids faible de l'adresse IP Multicast sont transférés dans les 23 bits de poids faible de l'adresse MAC.

Ainsi, pour l'adresse IP multicast 224.77.3.44, nous déterminons l'adresse MAC suivante :

Adresse IP sur 32 bits ==>	224	77	3	44
	1 1 1 0 0 0 0 0	1 0 0 1 1 0 1 0	0 0 0 0 0 0 1 1	0 0 1 0 1 1 0 0
		1 0 0 1 1 0 1 0	0 0 0 0 0 0 1 1	0 0 1 0 1 1 0 0
0 1 0 0	5 E	0 1 0 0 1 1 0 1	0 0 0 0 0 0 1 1	0 0 1 0 1 1 0 0
0 1 0 0	5 E	4 D	0 3	2 C

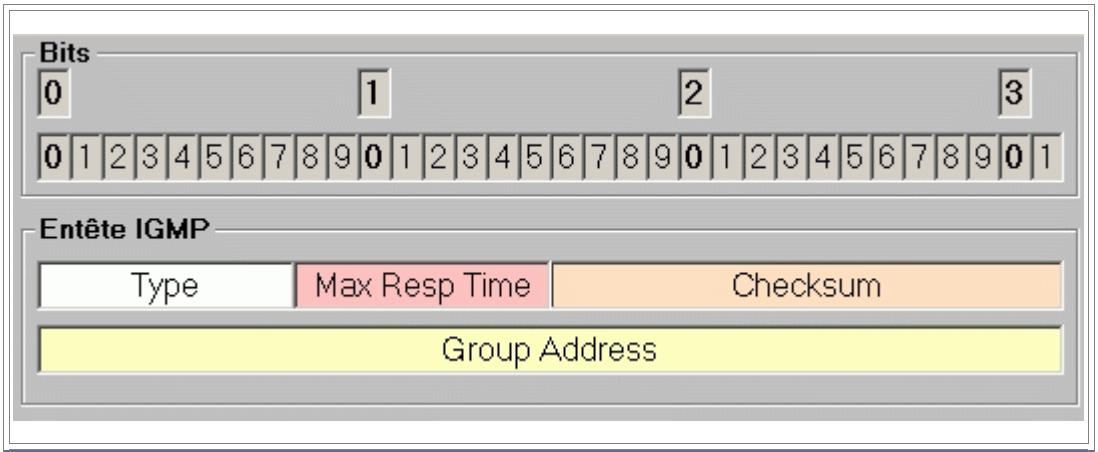
Dans notre cas, voici le mappage IP-MAC pour chaque adresse multicast utilisée :

IP	MAC
224.0.0.2	**01:00:5E:00:00:02**
224.77.0.0	**01:00:5E:4D:00:00**
224.77.1.0	**01:00:5E:4D:01:00**
224.77.3.44	**01:00:5E:4D:03:2C**

7.6 Structure d'une trame IGMP

IGMP est un protocole de niveau 3 (couche Réseau - OSI) qui fait partie intégrante de IP. Donc, la trame IGMP est encapsulée dans une trame IP comme les trames ICMP.

IGMP est identifié au niveau IP par la valeur **2** dans la zone ***Protocol***. Une trame IGMP est relativement simple :



Structure de l'entête IGMP

Le champ Type :

Elle détermine la nature du message IGMP. Il y a 3 types de messages.

- 0x11 : Requête pour identifier les groupes ayant des membres actifs.
- 0x12 : Rapport d'appartenance au groupe émis par un membre actif du groupe (IGMP version 1)
- 0x16 : Rapport d'appartenance au groupe émis par un membre actif du groupe (IGMP version 2)
- 0x17 : Un membre annonce son départ du groupe

Le champ Max Response Time :

Cette zone n'est utile que pour les messages de type 0x11. Elle indique le temps d'attente maximum pour un client avant l'émission du rapport d'appartenance. L'unité utilisée est le 1/10 de seconde. Pour les autres types de messages (0x11, 0x17) cette zone est initialisée à 0.

Le champ Checksum :

Somme de contrôle

Le champ Group Address :

Dans les messages de type 0x11, cette zone est à zéro quand le message IGMP ne concerne pas un groupe déterminé. Quand le message concerne un groupe identifié, cette zone contient l'adresse du groupe pour lequel on veut connaître l'existence de membres actifs.

Dans les messages de type 0x12, 0x16 ou 0x17, cette zone contient l'adresse IP du groupe concerné.