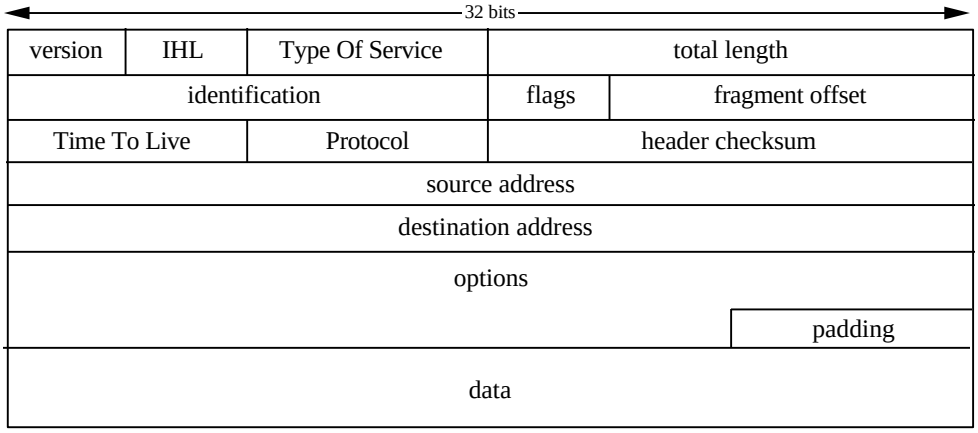
IP, Adressage, ARP, ICMP

Rappels

Format du datagramme IP



Dans le paquet IP, les champs ont la signification suivante

« version » définit le numéro de version du protocole IP utilisé. Actuellement, la valeur employée est « 4 » pour Ipv4.(4 bits)

« IHL » définit la longueur de l'entête. Cette valeur peut être différente entre deux paquets à cause du champs « options ».(4 bits)

« TOS » définit le type de service à appliquer au paquet en fonction de certains paramètres comme le délai de transit, la sécurité (8 bits).

« total length » définit la longueur du paquet (entête compris).(16 bits)

« identification » permet d'identifier de manière unique le paquet.(16 bits)

« flags » utilisé pour la fragmentation.(3 bits)

« fragment offset » précise la position du fragment si le paquet a été fragmenté (13 bits).

« TTL » « Time To Live » contient une valeur qui sera décrémentée à chaque passage dans un routeur. Si cette valeur atteint 0, alors le paquet doit être jeté, ceci afin d'éviter qu'un paquet ne circule « trop longtemps » au cas où il ne pourrait trouver son chemin et se serait mis à boucler.(8bits)

« Protocol » définit à quel protocole de niveau supérieur le paquet doit être remis.(8 bits)

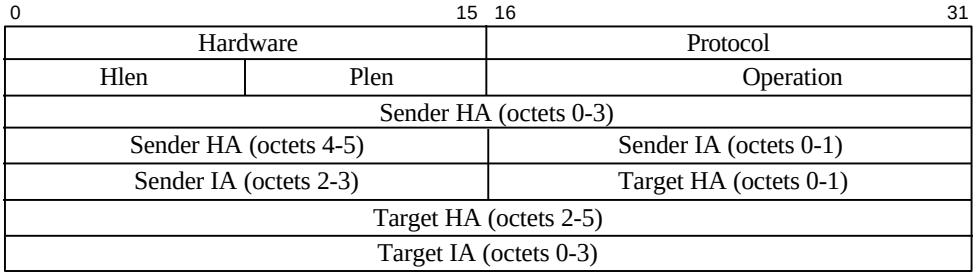
« header checksum » valeur de contrôle ne portant que sur l'entête. Doit être recalculé à chaque modification de TTL.(16 bits)

« source address » et « destination address » donnent les adresses sources et destination du paquet.(32 bits chaque)

« options » est un champ de taille variable qui inclut des informations sur le certains éléments de service que doivent mettre en œuvre les éléments de la communication pour répondre à certains besoins comme :le routage prédéterminé, la sécurité des données…

« padding » octets de bourrage afin de faire caler la fin de ce champ et des options sur un nombre entier de mots de 32 bits.

Le format du paquet ARP/RARP



0		15	16	31
Hardware			Protocol	
Hlen	Plen		Operation	
Sender HA (octets 0-3)				
Sender HA (octets 4-5)			Sender IA (octets 0-1)	
Sender IA (octets 2-3)			Target HA (octets 0-1)	
Target HA (octets 2-5)				
Target IA (octets 0-3)				

Hardware définit le type d'interface pour laquelle l'émetteur cherche une réponse

Protocol définit le type de protocole pour lequel une requête a été émise

Hlen définit la taille de l'adresse physique en octets

Plen définit la taille de l'adresse au niveau protocolaire

Operation décrit le type d'opération à effectuer par le récepteur

Sender HA définit l'adresse Hardware de l'émetteur

Sender IA définit l'adresse de niveau protocolaire demandé de l'émetteur

Target HA définit l'adresse Hardware du récepteur

Target IA définit l'adresse de niveau protocolaire demandé du récepteur.

1. TRAVAUX PRATIQUES : ANALYSE DE PROTOCOLES

1.1 – Démarrer la machine virtuelle vmware dans un terminal avec la commande suivante :

[user1@machine] $ vmware&

si nécessaire ajouter le chemin aux répertoires etc/sbin et /bin à la variable d'environnement PATH, en tapant la commande suivante :

[user1@machine] $ export PATH= "$PATH":/etc/sbin :/sbin

Lancer la machine virtuelle Serveur (FC5-ServerG) en sélectionnant la machine dans la liste (menu de gauche)

Connectez vous en tant qu'administrateur sur le serveur avec :

login = root
mot de passe = root.etu

Lancer la machine virtuelle Cliente (FC5-client) en sélectionnant la machine dans la liste (menu de gauche)

Connectez vous en tant qu'administrateur sur le client avec :

login = root
mot de passe = root.etu

1.2 : Compléter le tableau ci-dessous en utilisant la commande système dans un terminal sur les différentes machines (« Hôte », « Hôte virtuelle », « serveur virtuel », client virtuel»).

[user1@machine] $ ifconfig -a

Nom de la machine	interface	Adresse MAC	Adresse IP	Classe	Public/ Privée	Masque
Hôte	Eth0					
Hôte virtuel	Vmnet1					
Serveur virtuel	Eth0					
Client virtuel	Eth0					

1.2.c – Répondre aux questions suivantes :

- Combien de sous-réseaux différents pouvez vous identifier sur votre machine ?
- Quelle est la classe du sous-réseau auquel appartient le « Hôte » ?
- Combien de machines différentes peuvent être installées dans ce sous-réseau (hors interface du routeur) ?
- Quelle est la classe du sous-réseau auquel appartient les machines virtuelles ?
- Combien de machines différentes peuvent être installées dans ce sous-réseau (hors interface du routeur) ?

1.2.d - Vérifier au moyen de la commande « ping » la connectivité entre ces différentes machines et reporter vos résultats de tests dans le tableau ci-dessous :

	H	HV	SV	CV
H				
HV				
SV				
CV				

1.2.c – identifier le masque de sous-réseau. A quoi sert il ? Combien de bits sont ils utilisés pour numéroter les sous-réseaux ? Combien peut on avoir de stations (Interfaces adressables) au maximum par sous-réseau ?

1.2.d – Lancer l'analyseur de trafic WIRESHARK sur le poste Serveur au moyen de la commande suivante (dans un terminal) :

[user1@Serveur] $ ifconfig -a

Le programme « ping » sert à tester si une machine IP est bien accessible. La station émettrice génère un paquet ICMP « echo request » (type 8) et la station réceptrice renvoie un paquet ICMP « echo reply » (type 0). Les paquets ICMP sont encapsulés dans des datagrammes IP (champ protocole = 1). Au moyen de cette commande PING, tester la disponibilité du serveur. Décrire la

séquence d'échanges de trames observés entre le client et le serveur. Quels sont les protocoles de niveaux 2 et 3 qui sont mis en œuvre durant ces échanges ? Quelle est la valeur du champ « TYPE » au niveau Ethernet ?

1.2.e – A quoi sert le protocole ARP ? Peut on utiliser ce protocole avec une machine sur l'Internet ? Est il transporté dans un paquet IP ? Quelle est la valeur du champ « TYPE » au niveau Ethernet pour une trame ARP ? Comparer avec la question précédente ? A quoi sert donc ce champ « TYPE » ? Quelle est la valeur de l'adresse Ethernet destination utilisée par une requête ARP ? Est-ce une adresse de machine ?

1.2.f – Indiquer quels sont les champs de l'en-tête IP qui varient et ceux qui restent constants lors de l'échange induit par la commande PING ?

2. ADRESSAGE ET SUBDIVISION DE RESEAU

La subdivision de réseau est un procédé qui permet de découper logiquement des réseaux de grande taille en sous-réseaux de plus petites tailles. Pour ce faire, on applique, grâce à une formule mathématique, à partir d'une adresse de base, un masque de réseau. Le résultat est une plage d'adresses de machines continues mais de taille réduite par rapport à la plage d'adresses initiales.

2.1. L'adresse de la machine PC22 sur le site ie2 est 193.55.28.152. De quelle classe est cette adresse si on suppose qu'aucun sous-adressage n'a été appliqué par l'administrateur ? Quel est alors le masque du réseau ? Définir l'adresse de diffusion restreinte sur tout le réseau.

2.2 On désire subdiviser un réseau possédant le préfixe 129.178 en 60 sous-réseaux. Combien de machines au maximum pourra-t-on connecter sur chaque sous-réseau ? Quel sera le masque des sous-réseaux ?

2.3 Un réseau utilisant une suite d'adresses de classe B a un masque réseau égal à : 255.255.248.0. Ces trois stations d'adresses respectives : 129.148.208.26, 129.148.216.145 et 129.148.210.32 appartiennent-elles à ce sous-réseau ? Quelle est la plage d'adresses utilisée ? Définir l'adresse de diffusion restreinte.

3. FRAGMENTATION DES PAQUETS IP

2.4 Le sous-réseau 20 n'accepte que des paquets IP dont la taille ne dépasse pas 492 octets. Cette valeur est fixée par le format de trame utilisé pour transporter ces paquets.

Les autres sous-réseaux sont des LAN Ethernet dont la taille maximum de la trame est de 1518 octets.

Décrivez ce qui se passe aux niveaux Ethernet et IP, au passage de la passerelle B lorsqu'une trame de 1500 octets vient du réseau 10 pour aller vers le réseau 20.

U4. OUTILS SYSTEMES POUR LES RESEAUX

3.1 Que montrent les résultats des commandes "traceroute" suivantes.

```
traceroute to nephtys.lip6.fr (195.83.118.1), 30 hops max, 20 byte packets
 1 cisco1.ie2.u-psud.fr (193.55.28.33)             3 ms    2 ms    1 ms
 2 194.57.50.1 (194.57.50.1)                       6 ms   11 ms    2 ms
 3 195.83.240.209 (195.83.240.209)                 5 ms    3 ms    4 ms
 4 stlambert1.rerif.ft.net (193.48.53.221)        12 ms   14 ms    8 ms
 5 u-jussieu-paris-atm.rerif.ft.net (193.48.53.198)   19 ms   11 ms   10
ms
 6 r-jusren.reseau.jussieu.fr (134.157.255.126)   11 ms   11 ms   14 ms
 7 r-intercon.reseau.jussieu.fr (134.157.254.123)   10 ms   24 ms    6 ms
 8 nephtys.lip6.fr (195.83.118.1)                 10 ms    9 ms   10 ms
```

```
traceroute to rabelais.univ-tours.fr 193.52.209.14),30 hops max,20 byte
packets
 1 cisco1.ie2.u-psud.fr (193.55.28.33)             2 ms    2 ms    1 ms
 2 194.57.50.1 (194.57.50.1)                       3 ms    4 ms    5 ms
 3 195.83.240.209 (195.83.240.209)                 8 ms   10 ms    6 ms
 4 stlambert1.rerif.ft.net (193.48.53.221)         9 ms    6 ms    7 ms
 5 stamand1.rerif.ft.net (193.48.53.101)           5 ms    9 ms   11 ms
 6 nio-i.cssi.renater.fr (193.51.206.145)         12 ms   13 ms    7 ms
 7 nio-n1.cssi.renater.fr (193.51.206.9)          13 ms   14 ms   14 ms
 8 195.220.99.206 (195.220.99.206)                24 ms   18 ms   17 ms
 9 NRCP-orleans.cssi.renater.fr (195.220.99.34)   22 ms   17 ms   27 ms
10 NRCP-orleans.cssi.renater.fr (195.220.99.34)   20 ms   17 ms   24 ms
11 *
   tours.renacentre.ft.net (193.54.128.10)       240 ms  234 ms
12 u-tours.renacentre.ft.net (193.54.128.50)     316 ms  269 ms  330 ms
13 193.52.208.11 (193.52.208.11)                 441 ms  382 ms  355 ms
14 193.52.209.62 (193.52.209.62)                 417 ms  321 ms  436 ms
15 rabelais.univ-tours.fr (193.52.209.14)        506 ms  539 ms  608 ms
```

3.2 Que se passe-t-il lorsqu'un datagramme IP arrive dans un routeur avec un champ « durée de vie » (TTL) à 1 ?