Licence 3 de Sciences, mention Informatique

Réseaux et Protocoles

Modèle de document pour un rapport d'étude

Présenté par

Julien Montavont

montavont@unistra.fr

Contents

1 Introduction

2 Concepts et utilisation

2.1 En-tete IPv4

Un packet IPv4 est precede‘ par un en-tete ayant une longeur minimale de 20 octets (dans les cas aucune option supplementaire a ete specifie‘). La figure suivante montre le contenu de l'en-tete d'un packet IPv4.

TODO FIGURE

Comme on peut voir dans la figure ci dessus, un en-tete IPv4 est compose‘ par 13 champs. En realite nous verrons plus loin que cet en-tete peut, quand il est necessaire, contenir un champ additionel qui servira a specifier quelque option qui n'est pas presente dans le 13 champs ci dessus.

Commencons par voir plus en detail les 13 champs d'un en-tete IPv4 standard:

Version Cette champ occupe les premiers 4 bits de l'en-tete IPv4. Il est utilise pour determiner le type de protocole utilise‘ par la couche reseau (chouche 3). Dans le cas de IPv4 cet champs contiendra toujours la valeur 4, qui justement identifie le protocole IPv4.

Cet champ n'est pas tres utilise, en tenant compte que le protocole a utiliser pour la couche 3 est presque toujour specifie dans l'en-tete de la couche liason.

IHL Le champ IHL specifie la taille de l'en-tete IPv4, en fait IHL est l'acronime de Interet Header Length. Bien entendu, en disant cela on souligne un concept important a propos du protocole IPv4: la taille de l'en-tete n'est pas fixe.

La taille de l'en-tete est exprime‘e en bloques de 32 bits. Etant donne une taille de 4 bits pour le champ IHL, la longueur maximale d'un en-tete IPv4 est de 15 bloques de 32 bits, qui correspond a 60 octets. Comme l'en-tete IPv4 a une taille minimale de 20 octets (160 bits), le champ IHL ne peut pas contenir un valeur inferieure a 5.

Type of Service Le champ Type of Service, mieux connu avec l'acronime ToS, est utilise pour specifier la qualite de service souhaite pour l'envoi d'un packet IPv4. Cet champ occupe un octet de l'en-tete et il se compose en trois parties. Une premiere partie de 3 bits permet d'indiquer la precedence avec la quelle le packet doit etre traite, les 3 bits apres sont utilise pour specifier certaines caracteristiques du service, notament: le temp, le debit et la fiabilite. Enfin l'emploi des 2 derniers bits n'a pas ete specifie et leur usage a ete laisse libre pour des implementationes futures.

En realite l'histoire de cet champs est bien plus longue et complexe que ca, car en pratique la facon d'utiliser cet champs a ete modifie plusieurs fois au cours des annees. [1] Cette manque de stabilite a par fois cause une certaine confusion dans les implementations. [2]

Aujourd'hui les 8 bits du champ ToS sont utilise par le mecanisme DiffServ (Differentiated Services). Cet systeme utilise les premieres 6 bits du champ ToS (DSCP - Differentiated Services Code Point) pour marquer chaque paquet comme appartenant a un niveau de priorite et une classe de service. Chaque classe determine le type de traitement que on souhaite demander pour le paquet aux routers au long du chemin (PHB - Per-Hop behaviour), toutefois le service offert par chaque router est fortement lie a sa configuration. [3] Le dernieres 2 bits du champ ToS sont utilise pour l'extension ECN (*Explicit Congestion Notification*). Cette extension, propose par RFC2481 et introduite deux annees apres avec le RFC3168, ajoute un systeme de controle de la congestion du traffic reseau. Dans le cas d'une saturation de la reseau cet champ est utilise pour notifier cet probleme et demander a le dispositif emetteur une reduction du rythme au quel les packets sont envoye, avec l'objectif de reduir l'attente et la perte de packets.

Total length Comme le suggere le nom, ce champs est utilise pour indiquer la taille totale du packet IPv4: en tete plus donnes. Le champ *Total length* est defini sur 16 bits, ceci permet de indiquer un valeur compri entre 0 et 65,535 octets. Comme l'en-tete est compris dans la longeur totale d'un packet cet valeur ne sarait jamais inferieur a 20 (taille minimale d'un en-tete IPv4 en octets). RFC 791 impose a toutes les dispositifs d'une reseau IPv4 la capacite de recevoir des packets jusq'a une taille de 576 octets, cette prerogative permet de eviter une excessive fragmentation.

Identification Cet en-tete (sur 16 bits) permet d'identifier les fragments appartenent au meme packet.

Flags Le 3 bits du champs Flags sont utilise pour gerer la fragmentation d'un packet. Un de ces bit est emploie pour indiquer si le paquet peut etre fragmente ou non. Cet bit, appelle DF (*Don't Fragment*), doit etre pris en consideration par les routers dans le chemin pour decider si un paquet trop grand pour etre trasmis peut etre retrasmis sous forme de fragments plus petits ou rejete. Un autre bit, appelle MF (*More Fragments*), indique si le paquet est suivi par d'autres fragments. Le bit MF est mis a 0 dans le dernier fragment ou dans des paquet qui n'ont pas ete fragmente.

Un des trois bits de ce champs n'est pas actuallement utilise mais il a ete reserve pour applications futures possibles. [4]

[1] L'utilisation des 8 bits du champ ToS a ete redefinie par cinq standard differents (plus divers standars experimentals). Les documents presentent ces standard sont mentionne dans le chapitre "Historical Definitions for the IPv4 TOS Octet" du RFC 3168

[2] Comme le souligne le RFC 3260 *"At least one implementor has expressed confusion about the relationship of the DSField, as defined in RFC 2474, to the use of the TOS bits, as described in RFC 1349"*

[3] *"The DiffServ standard does not specify a precise definition of "low," "medium," and "high" drop probability. Not all devices recognize the DiffServ (DS2 and DS1) settings; and even when these settings are recognized, they do not necessarily trigger the same PHB forwarding action at each network node. Each node implements its own response based on how it is configured."* - Implementing Quality of Service Policies with DSCP http://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html

[4] Cet bit a ete aussi le protagoniste d'un des plus connu poissons d'avril presentee par le IETF. Pour faciliter

Fragment Offset Lorsque un paquet a ete fragmentee cet en-tete est utilisee pour determiner la position (offset) d'un fragment par rapport a les donnees du paquet reassemble. Le decalage de chaque fragment est exprime en bloques de huit octets (ou 64 bits). Le champ Fragment Offset utilise 13 bits de l'en-tete IPv4, cela permet un offset maximale de 65,528 octets.[5] Etant donne que la flag MF (*More Fragments*) doit etre mise a zero lorsque si un paquet n'est pas fragmentee ou si il est le dernier fragment d'un paquet plus grand, l'unique difference entre ce deux types de paquets est le valeur de le champ Fragement Offset que, dans le cas d'un paquet pas fragmentee, est toujours zero.

Time to Live Cet champ determine le nombre maximal de fois qu'un paquet peut etre retrasmis, il est utilise pour empecher que un paquet puisse etre retrasmis a l'infini. Chaque router au long du chemin d'un paquet est tenu a detruir un paquet si le valeur du TTL (*Time to Live*) est zero ou decrementer cet champs par le nombre de secondes que le paquet passe en attente d'etre trasmis.

En theorie le TTL indique le nombre de secondes pendant le quels un paquet peut continuer a etre retrasmis dans une reseau ,mais , etant chaque router toujour tenu a decrementer cet champ de au moins 1 (meme si le paquet a ete retrasmis en moin qu'un seconde) et considerant les performances des routers d'aujourd'hui, en pratique le TTL indique le nombre maximum de router que un paquet peut incontrer au long de son chemim.

Le space reservee au TTL dans l'en-tete IPv4 est de un octet ce que comporte un TTL maximum de 255.[6]

Quand un paquet a ete detruit ensuite a l'expiration du TTL, le router qui a detruit le paquet peut decider de envoier un message d'erreur a l'emetteur du paquet detruit. Cet type de message (ICMP Time exceeded) est utilise par utils comme *traceroute* pour decouvrir, approximativement, le chemin d'un packet IP.

Protocol Chaque paquet IPv4 specifie le protocole utilise par les donnes trasmises: cela est l'objectif de ce champs de 8 bits

Header Checksum Cet champ contient une somme de controle et est utilise pour detecter des erreurs dans l'en-tete IPv4. Le valeur de cet champs est recalcule at chaque retrasmission[7]: si il ne correspond pas avec celui presente dans l'en-tete le paquet est detruit.

3 Suite de protocole

3.1 ARP

ARP (Address resolution protocol) est un protocole à cheval sur la couche 2 et la couche 3. La fonction principale d'ARP est de faire la conversion entre les adresses de niveau 2 et de niveau 3. Cela est très utilisé étant donné que les hôte connaissent souvent les adresses IP de leur destinataire, mais rarement l'adresse de niveau 2 de ce destinataire ou de la passerelle à contacter pour joindre le destinataire.

3.1.1 Exemple

Dans la partie qui suit nous allons nous placer dans l'exemple suivant. TODO LAN exemple

les taches des systems de filtrage le RFC 3514 propose d'utiliser ce bit pour etiqueter paquets mailveillant, a ce titre tous les paquets etant envoye avec ce bit (renomme "*Evil Bit*") mis a 1 seront mis a la poubelle.

[5] En pratique un tel offset n'est jamais utilisee car, en ajoutant un en-tete minimale de 20 octets, la taille totale du paquet reassemble depaserait la longeur maximale d'un paquet IPv4.

[6] Le RFC 1700 recommende un valeur par defaut de 64.

[7] Cela est necessaire car le TTL est decrementee at chaque retrasmission et un changement de l'en-tete comporte un valeur different dans la somme de controlle

3.1.2 Entête

3.1.3 Fonctionnement

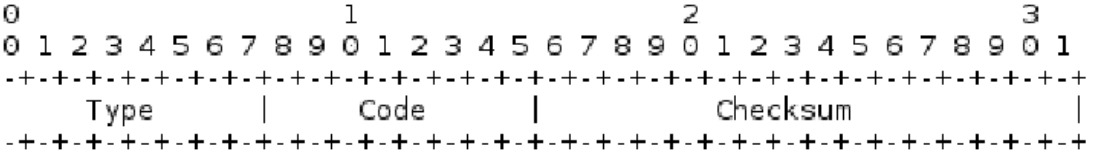
Prenons l'exemple où A veux envoyer un message à B. A connait l'adresse IP de B. Donc A va préparer son paquet qu'il va envoyer à B, avec son adresse IP en source et l'adresse IP de B en destination. La paquet passe dans la couche liaison, il va être enpaqueté dans une trame de niveau 2. Cette trame aura comme adresse source l'adresse de niveau 2 de A, mais à ce moment il ne peux pas completé l'adresse destination de la trame: en effet, il ne connait l'adresse de niveau 2 du destinataire. La paquet reste bloqué en couche 2 et ne peux pas être envoyé au destinataire. Comment obtenir l'adresse de niveau 2 du destinaire? Le protocole ARP est capable de faire cette translation.

3.1.4 ACD

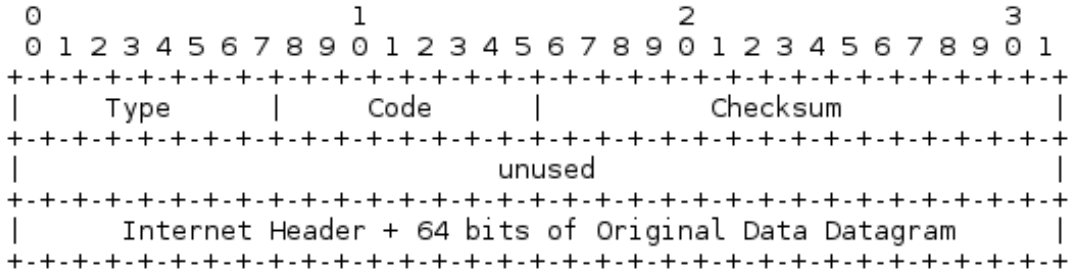
Adresse conflict detection

3.2 ICMP

ICMP (Internet Control Message Protocol) est un protocole de niveau 3 faisant partie intégrante du protocole IPv4. Il permet de transmettre des informations de controle et d'erreur. Les messages ICMP sont empaquetés dans des paquets IP, ils diposent donc d'un entête de paquet IP. Cet entête est le même que pour tout les autres entêtes de paquet d'IPv4. Deux champs son intéressant dans le cas d'un paquet ICMP, les champs Protocol et Type of service. Le champ Protocol est mis à à la valeur 1 pour dire que le paquet contient un message ICMP, et le champ ToS est mis à 0 //TODO(pourquoi 0?)//. Après le header du paquet IPv4, commence la partie data qui contient le message ICMP. Ce message contient des champs différent en fonction du type de message à passer. Cependant les trois premier champs sont toujours les mêmes. Les types de messages ICMP qui vont suivrent sont ce décrit dans la RFC 792.[8]



Le premier champ est celui de type. Il permet, premièrement, de donner le type du paquet et de l'information à transmettre, et deuxièmement de préciser la nature des champs qui vont suivres. En effet, comme vu plus haut, les messages contiennent des champs différents selon le type du message ICMP.
Le deuxième champ est le code. Il permet de subdiviser le type en donnant des détails plus précis.
Enfin le troisième champ est la somme de contrôle (checksum)//TODO(plage de controle).
Commençons avec les messages qui possèdent l'ensemble de champs le plus simple.



Les messages qui utilisent cette organisation sont les messages de type 3, 4 et 11.

[8] https://tools.ietf.org/html/rfc792

3.2.1 Message de type 3: Unreachable Destination

Les messages de type 3 sont émis lorsqu'un paquet n'a pas réussi à joindre la destination (Unreachable destination). Cette erreur peux être dut à plusieurs facteurs, et les codes permettent de préciser pourquoi le paquet n'a pas pu rejoindre sa destination.

Code 0

3.2.2 Message de type 4:

3.2.3 Message de type 11: Time Exceeded

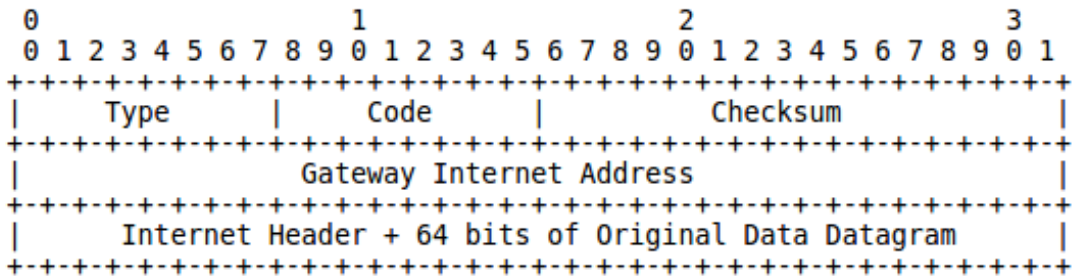
Ces messages sont envoyés lorsque le TTL d'un paquet à atteind 0. Une autre utilisation des ces messages est lorsque que le temps de ré-assemblage des fragments d'un paquet est dépassé. Ces deux cas sont distingé par le code. Ces messages ont pour destinataire l'hôte qui à envoyé le paquet qui à provoqué l'erreur.//TODO(vérifier) Le champ Internet header contient l'entête du paquet qui a été supprimé plus les 64 bits suivant celui-ci. Cela permet à l'émetteur de retrouver quel paquet à été supprimé.

Code 0: Le code 0 est utilisé pour indiquer que le TTL du paquet posant problème est arrivé à 0. Lorsque le TTL d'un paquet arrive à 0, celui-ci est supprimer et un message ICMP de type 11 et de code 0 est envoyer par le routeur qui à détécté le problème. Cela permet principalement d'éviter qu'un paquet sans dans une boucle et qu'il soit rélayé à l'infini.

Code 1: Le code 1 est quant à lui utilisé pour indiquer //TODO

3.2.4 Message de type 5:

Les message de type 5 utilisent les entêtes ci-dessous et servent à faire de la redirection. En effet, lorsqu'un routeur détecte que le prochain routeur dans lequel va transiter le paquet se trouve dans le même réseau que l'émetteur de ce paquet, il va envoyer un message ICMP pour avertir cet hôte (et/ou le réseau) qu'il existe un chemin plus court en envoyant directement les paquets vers le prochain routeur. Ce message ICMP va avoir pour effet de modifier la table de routage interne à l'émetteur (et/ou des hôtes connecté au réseau). Concernant le paquet que le premier routeur à reçu, il va le transmettre vers sa destination.



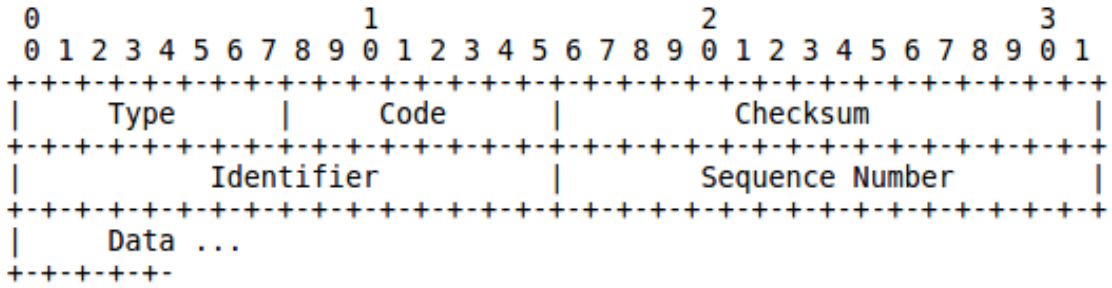
Le champ Gateway Internet Address contient la l'adresse du routeur auquel il faut faire transiter le traffique directement pour avoir un chemin de routage plus court. Le champ Internet Header contient toujours l'entête du message ayant porvoqué l'envoie du message ICMP plus les 64 bits suivant l'entête. Cela permet à (aux) hôte(s) de pouvoir modifier leur table de routage en fonction la destination que cherchait à atteindre le paquet.

Code 0 Ce code indique que la redirection est adresser à tout le réseau de l'émetteur du paquet.

Code 1 Ce code indique que la redirection est adresser à l'émetteur du paquet.

Code 2 Ce code indique que la redirection est adresser à tout le réseau de l'émetteur du paquet et aux services(//TODO(préciser)).

Code 3 Ce code indique que la redirection est adresser à l'émetteur du paquet(//TODO(préciser)).



3.2.5 Message de type 8 et 0:

Les messages de type 8 et 0 servent à faire des envoies et des renvoies d'information. Les messages de type 8 font des envoies d'informations, appelé echo request. Tandis que les messages de type 0 sont envoyés en réponse aux echo request et renvoie les informations reçus de ceux-ci; ils sont appelés echo reply. Etant donnée que les echo reply sont des réponses aux echo request, l'adresse destination des echo reply est l'adresse source des echo request. Ces deux messages peuvent envoyés et reçu aussi bien par un hôte que par un routeur. Ce sont notamment les message envoyés par la commande *ping* qui permet de vérifier si l'on peux communiquer avec un hôte ou un routeur. Les champs Identifier et Sequence Number aide l'émetteur de l'echo request à associer les echos request qu'il à envoyés avec les echos reply qu'il à reçus. //TODO(qui a t-il dans data?)

3.3 IGMP

3.4 DHCP

4 Conclusion