TP 3 de Réseaux en L3 Informatique : Outils de capture de paquets et Analyse de trames (Ethernet, ARP, ICMP, DHCP), Tables ARP, attribution dynamique d'adresses IP

Auteur : Olivier GLÜCK, Université Lyon 1

Objectifs

- utilisation de `tcpdump` et `wireshark`
- observation des protocoles ARP, ICMP et DHCP
- analyse de trames Ethernet
- installation et configuration d'un serveur DHCP
- utilisation d'un miroir debian pour l'installation de packages

Pré-requis

Adressage IP, configuration réseau des machines, utilisation d'un miroir debian pour l'installation de packages

1. Introduction (pour vous aider !)

1.1. Outils de capture de paquets

Pour communiquer, les machines échangent des informations sous forme de paquets qui sont l'unité de données échangées sur le réseau. Il est possible « d'écouter » le câble Ethernet et de regarder ce qui se passe quand vous lancez des commandes comme `ping`, `rlogin`, …

Un premier outil permettant d'observer le réseau s'appelle `tcpdump`. Pour écouter le trafic sur l'interface `eth0`, il faut taper la commande `tcpdump -i eth0`. Par défaut, `tcpdump` écoute en « *promiscuous mode* », c'est à dire qu'il capture et analyse toutes les trames circulant sur le réseau même celles qui ne concernent pas la machine sur laquelle il tourne.

Un deuxième outil, un peu plus convivial que `tcpdump` car utilisable en mode graphique avec un affichage plus lisible, est l'utilitaire `wireshark`. N'oubliez pas de cocher « `Update list of packets in real time` ».

Ces deux outils permettent d'établir des filtres de capture de paquets de manière assez fine. La syntaxe des filtres utilisés et la même pour `wireshark` que pour `tcpdump`. Par exemple, la commande `tcpdump -i eth0 tcp dst port 53` permet de ne capturer sur l'interface `eth0` que les segments TCP dont le port de destination est 53. Pour plus d'informations, consultez la page manuelle de `tcpdump`.

1.2. Comment installer un nouveau package ?

1- Exécutez la commande `apt-get update` en tant qu'administrateur dans un terminal et vérifiez que tout se passe bien (il ne doit pas y avoir de message d'erreur).
2- Désormais, vous pouvez installer un package à partir du serveur ftp/http d'Internet :
`apt-get install nom_pkg` où nom_pkg est le nom du package à installer
Pour ce TP, les packages qui nous intéressent sont :
`telnetd` (serveur DHCP), `dhcp3-server` (serveur DHCP), `dhcp-client` (client DHCP), `dhcpdump` (capture des trames dhcp)
3- Pour vérifier que le package est correctement installé, faire un `dpkg -l`

1.3. Commandes et fichiers à utiliser

PENSER A UTILISER LES PAGES MANUELLES DE LINUX :
`man <nom de la commande>`

- `ifconfig <interface> <adresse> netmask <adresse du mask> broadcast <adresse broadcast>`
- `ping` et `pong`
- `/etc/network/interfaces`
- `/etc/hosts` – permet de nommer symboliquement les machines
- `/etc/networks` – permet de nommer symboliquement les réseaux
- `netstat` – permet de visualiser la table de routage d'une machine
- `route –` permet de configurer la table de routage d'une machine
- `arp –` permet de visualiser la table ARP d'une machine
- `tcpdump` et `wireshark` pour capturer des paquets sur le réseau
- `apt-get` pour installer un package
- les fichiers suivants concernent le client ou serveur DHCP
  - `/etc/default/dhcp3-server` fichier de config du serveur DHCP
  - `/etc/dhcp3/dhcpd.conf` fichier de config du serveur DHCP
  - `/var/lib/dhcp3/dhcpd.leases` fichier de log du serveur DHCP
  - `/etc/dhclient.conf` fichier de config du client DHCP
  - `/etc/dhclient-script` script associé au client DHCP

2. Utilisation de `tcpdump` et `wireshark`

Pour cette partie, regroupez vous à deux ou trois binômes (il faudra utiliser une machine source, une machine destinataire et une machine exploratrice pouvant communiquer entre elles).

2.1. Découverte d'un mot de passe

Manipulation

Créez un compte utilisateur sur une machine avec la commande `adduser`. Entrez un mot de passe que vous allez ensuite essayer de capturer. Sur cette même machine, installez le package `telnetd`. Lancez `tcpdump` et/ou `wireshark` sur une deuxième machine. A partir d'une troisième machine, ouvrez une connexion distante vers la machine sur laquelle vous venez de créer le compte, en tant que l'utilisateur nouvellement créé. Vous pouvez

utiliser par exemple `rlogin` *et/ou* `telnet`*. Analysez les trames capturées et essayez de retrouver le mot de passe de l'utilisateur. Essayez maintenant la même manipulation en utilisant* `ssh` *pour réaliser la connexion à distance. Quel est l'intérêt de* `ssh` *? A la fin de la manipulation, effacez le compte utilisateur avec* `deluser`*.*

2.2. Analyse de protocoles (ICMP et ARP)

Manipulation

Effacez toutes les entrées présentes dans la table ARP à l'aide de la commande `arp`*. Lancez* `wireshark` *sur la machine exploratrice et faites un* `ping` *entre la machine source et la machine destination. La commande* `ping` *utilise le protocole ICMP pour contacter la machine distante et le protocole ARP pour obtenir l'adresse Ethernet de la machine distante. Décrivez à l'aide d'un chronogramme et expliquez l'enchaînement dans le temps des paquets échangés. Retrouvez dans le format hexadécimal, les valeurs des différents champs (en-tête Ethernet, données ARP, …).*

Manipulation

Videz les tables ARP de la machine source (A) et de la machine destination (B). Faire un `ping` *de A vers B. Consultez les tables ARP. La table de B contient-elle l'adresse de A ?*

Question

Qu'est-ce qui permet d'identifier les paquets comme étant de type ARP ou ICMP ? Les paquets ARP ou ICMP sont-ils encapsulés dans des paquets IP ? Quel est le rôle des différents champs ARP ? Quel est le format d'une trame Ethernet ? Comment le niveau Ethernet détermine t-il la fin du paquet ? Faites un schéma comportant les différents protocoles examinés et montrant les différents niveaux d'encapsulation des protocoles les un dans les autres. Faites également un schéma correspondant au format des paquets ARP observés.

Manipulation

Utilisez les options `-s` *puis* `-p` *de* `ping` *et analysez le comportement au niveau du contenu des paquets échangés.*

3. Attribution dynamique d'adresses IP (DHCP)

DHCP est un protocole qui permet de configurer automatiquement les paramètres réseau des machines lors de leur démarrage (adresses IP, netmask, dns, passerelle, …). Cela évite de mettre les configurations du réseau « en dur » sur les postes connectés.
Pour plus de souplesse, nous souhaitons dans cette section attribuer dynamiquement les adresses IP des machines. Pour attribuer automatiquement les configurations IP des ordinateurs d'un réseau, il suffit d'installer et de configurer un serveur DHCP puis d'indiquer aux machines clientes de contacter le serveur pour se voir attribuer une configuration IP.

Pensez à utiliser les pages man suivantes :
page de manuel `dhcpd` — décrit le fonctionnement du démon DHCP
page de manuel `dhcpd.conf` — explique comment configurer le fichier de configuration DHCP ; comprend des exemples
page de manuel `dhcpd.leases` — explique comment configurer le fichier d'attribution DHCP ; comprend des exemples

page de manuel `dhcp-options` — explique la syntaxe de déclaration des options DHCP dans `dhcpd.conf` ; comprend des exemples

3.1. Configuration d'un serveur DHCP

Manipulation

Exécutez la commande suivante : `touch /var/lib/dhcp3/dhcpd.leases`
Installez le package `dhcp3-server`*. Configurez votre machine pour qu'elle soit serveur DHCP en créant/modifiant les fichiers* `/etc/default/dhcp3-server` *et* `/etc/dhcp3/dhcpd.conf` *; le premier fichier permet d'indiquer au serveur DHCP les interfaces réseaux sur lesquelles le serveur DHCP doit écouter ; le deuxième fichier permet de configurer le serveur (*`man dhcpd.conf`*) : adresse de sous-réseau, adresse de broadcast, adresse de la passerelle, durée de vie de l'adresse IP attribuée au client, plage d'adresses IP attribuables par le serveur,… Vous pouvez aussi vous inspirer du fichier exemple.*

3.2. Configuration d'un client DHCP

Manipulation

Installez le package `dhcp-client`*. Configurez votre machine en tant que client DHCP afin qu'elle récupère sa configuration réseau sur un serveur DHCP voisin. Pour ce faire, vous devrez modifier le fichier* `/etc/network/interfaces`*.*

3.3. Tests et observations

Manipulation

Lancez un des serveurs DHCP du sous-réseau (`/etc/init.d/dhcp3-server start|stop|restart`*) et redémarrez la configuration réseau sur les machines clientes (*`/etc/init.d/networking start|stop|restart`*).*
Vérifiez le bon fonctionnement du serveur DHCP en consultant les messages de log (`tail -f /var/log/syslog`*). Vous pouvez aussi lancer le serveur en premier plan en mode debug (options* `-f -d` *).*
Faites varier les paramètres du serveur (plage d'adresses, `default-lease-time`*) et observez le bon fonctionnement. Testez tour à tour votre serveur DHCP.*

Question

Que contient le fichier `/var/lib/dhcp3/dhcpd.leases` *?*

Manipulation

Regardez avec `wireshark` *les trames DCHP échangées. Quels sont les différents types de message du protocole DHCP ? Essayez de capter les messages* `DHCPDiscover` *et* `DHCPOffer` *en redémarrant le réseau sur le client DHCP.*

Question

Rajoutez pour chaque sous-réseau une ligne du type `option routers` *… dans le fichier de configuration du serveur DHCP. Quelle est l'incidence sur les tables de routage des machines clientes ?*

Question

Comment attribuer toujours la même adresse IP à un client selon son adresse MAC ?

Manipulation

S'il reste du temps, regardez comment configurer plus précisément le client (`man dhclient.conf`) et testez certaines options. Installez et utilisez le package `dhcpdump`.

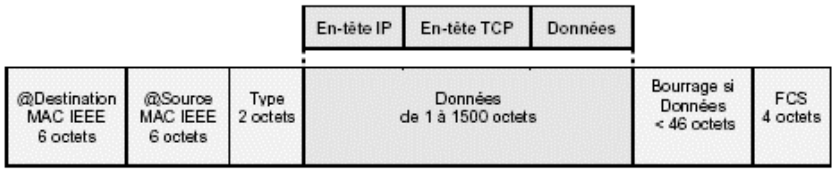
4. Annexes

Exemple de configuration `/etc/dhcpd.conf`

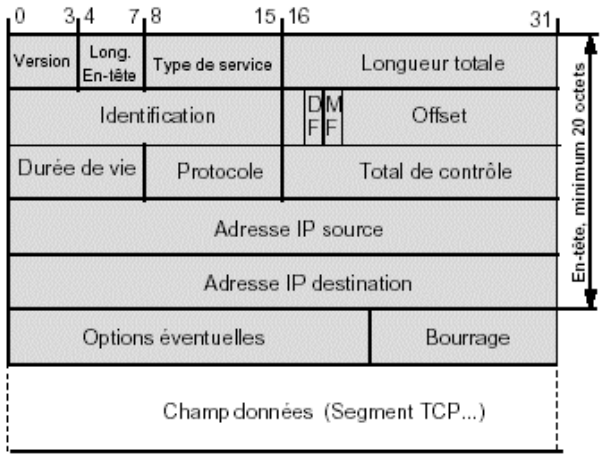
```
# Pour que le lease fonctionne (voir http://www.isc.org/index.pl?/sw/dhcp/authoritative.php)
authoritative ;

# On donne le nom du domaine
option domain-name "nom_choisi";

#On défini le masque réseau
option subnet-mask 255.255.255.0;

# Ici c'est le serveur de nom, le serveur privé,
# il faut aussi mettre le/les DNS donnés par votre provider.
option domain-name-servers 192.168.1.2 , 192.168.1.3;
ddns-update-style ad-hoc;

# Les clients auront cette adresse comme passerelle par défaut
option routers 192.168.1.1;

#Le bail a une durée de 86400 s par défaut, soit 24 h
# On peut configurer les clients pour qu'ils puissent demander une durée de bail spécifique
default-lease-time 86400;

#On le laisse avec un maximum de 7 jours
max-lease-time 604800;

# Définition du réseau : 192.168.1.0 et de son masque
subnet 192.168.1.0 netmask 255.255.255.0 {

#La plage d'adresses disponibles pour les clients
range 192.168.1.4 192.168.1.253;

# Et l'adresse utilisée pour la diffusion
option broadcast-address 192.168.1.255;
}
# Définition de notre machine PC-1
host PC-1 {
option host-name "machinePC1";
hardware ethernet 00:00:4C:71:46:68;
fixed-address 192.168.1.5;
}
```



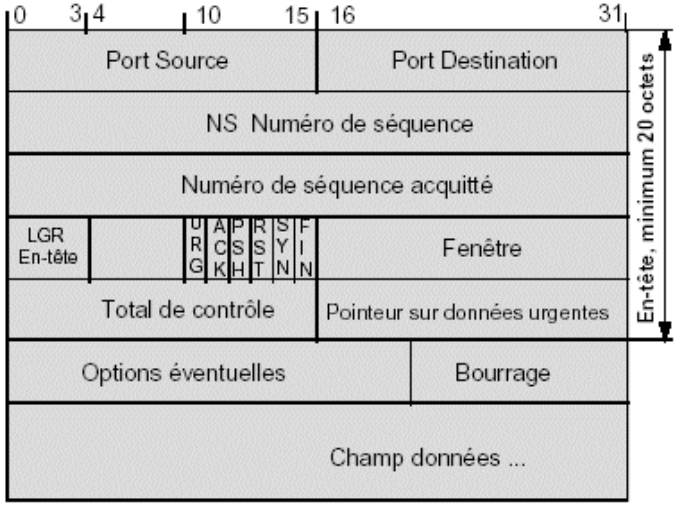
```
# Exemple d'un réseau avec plusieurs sous réseaux
shared-network nom {
   option domain-name              "test.redhat.com";
   option domain-name-servers      ns1.redhat.com, ns2.redhat.com;
   option routers                  192.168.1.254;
   plus de paramètres pour EXEMPLE de réseau partagé
   subnet 192.168.1.0 netmask 255.255.255.0 {
      paramètres pour sous-réseau
      range 192.168.1.1 192.168.1.31;
   }
   subnet 192.168.1.32 netmask 255.255.255.0 {
      paramètres pour sous-réseau
      range 192.168.1.33 192.168.1.63;
   }
}
```



Format de la trame Ethernet v2 et encapsulation IP.

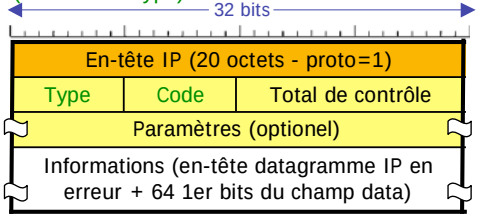


Format du datagramme IP.



Format du segment TCP.

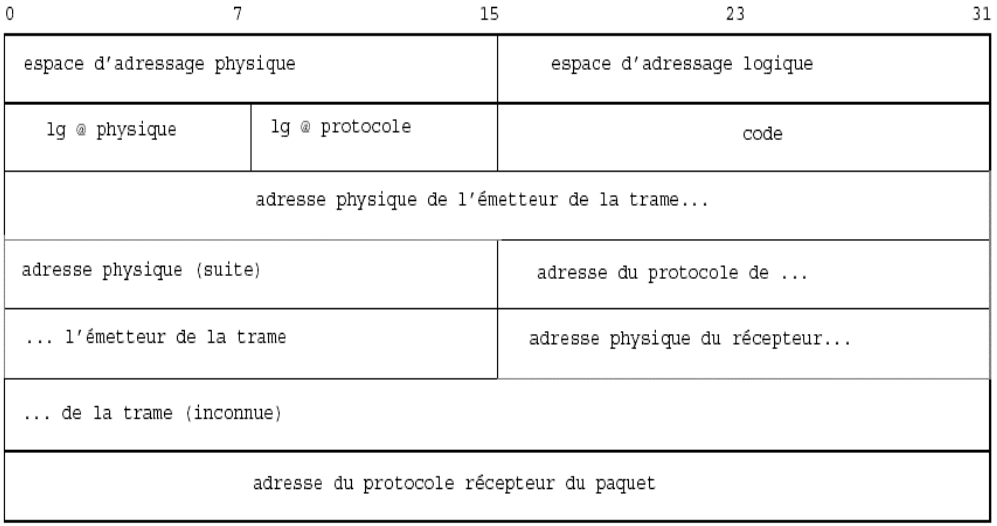
Le champ Code : code d'erreur (fonction du type)



Le champ Type :

- 0 : réponse d'Echo
- 3 : destination inconnue
- 4 : limitation du débit par la source
- 5 : redirection (ICMP redirect)
- 8 : demande d'Echo
- 11 : expiration de délai (TTL=0)
- 12 : en-tête IP invalide
- 13/14 : requête/réponse d'horodatage
- 17/18 : requête/réponse de netmask

Format d'un paquet ICMP



Format d'un paquet ARP