IUT du Limousin
Département Informatique
M2102/2016/TD3/ER/

M2012 - TD3

IP & ICMP

1. Le protocole ICMP

1.1. Problématique

IP étant fondamentalement un protocole non fiable, un mécanisme a donc dû être mis en place de manière à informer des différents problèmes pouvant survenir sur le réseau. Il s'agit du protocole ICMP (pour Internet Control Message Protocol), qui fait partie intégrante de la couche IP.

Lorsqu'un incident est détecté, la machine (un routeur en général) qui le détecte informe la machine à l'origine du message du problème et éventuellement de l'action entreprise. Par exemple, lorsque le TTL d'un paquet IP arrive à 0, le routeur détruit le paquet et envoie alors le message correspondant à l'expéditeur du paquet détruit (message ICMP type 11).

1.2. Types de message

Il existe donc un grand nombre de types de message différents, mais tous respectent le format présenté ci-dessous. Les messages ICMP sont alors différenciés par leur champ *Type de message*, et le *Code* associé.

Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
Type de message	Code	Somme de contrôle	
Bourrage ou données			
Données (*optionnel et de longueur variable*)			

Fig. 4. Format du message ICMP

Le message ci-contre consitue alors la partie DATA d'un paquet IP. Le code associé au protocole ICMP au niveau du paquet IP est `0x01`.

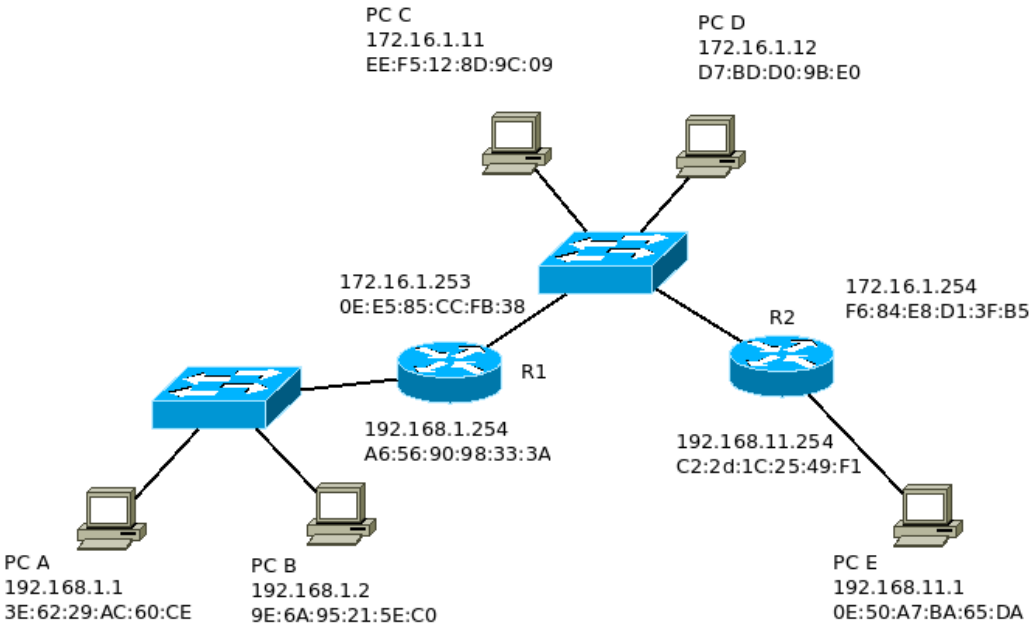
Parmi les messages les plus courants, on peut notamment citer :

- **type 8** et **type 0** : messages « ping » (question et réponse),
- **type 3** : destination inacessible,
- **type 11** : délai dépassé (TTL à 0).

2. Exercices

2.1. Analyse d'erreurs

Pour tout l'exercice, on considérera le réseau ci-dessous.

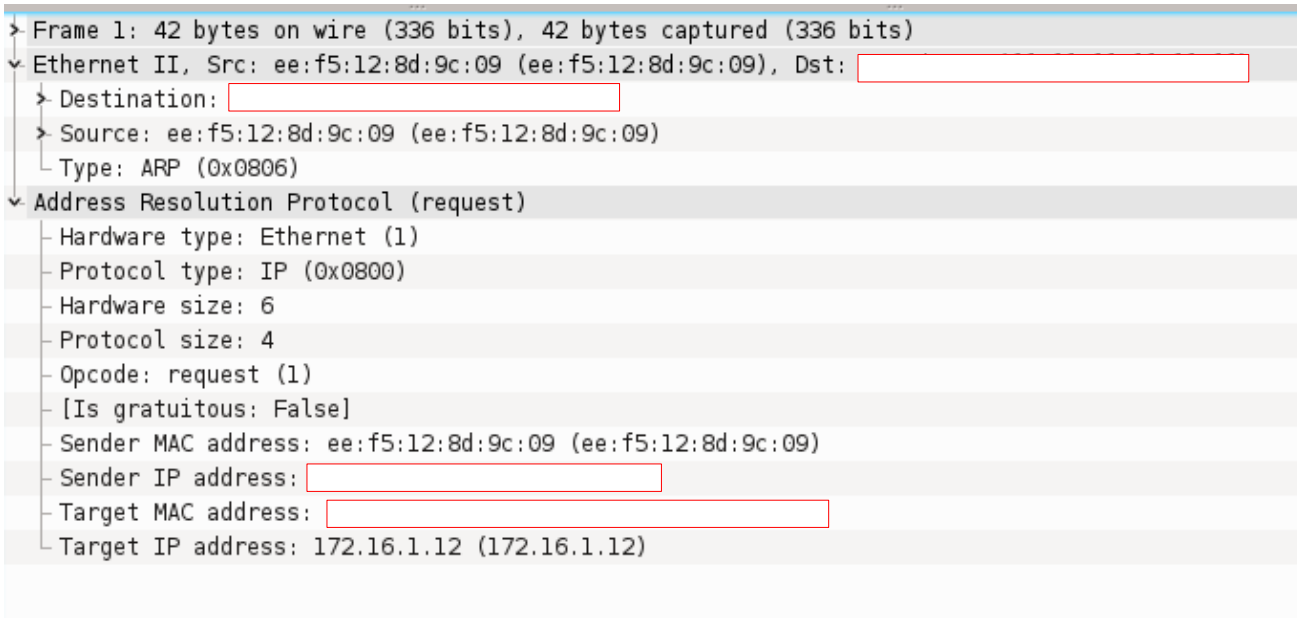


1. Complétez la trame ci-dessous, et indiquez quelle commande a été utilisée, en précisant sur quelle machine.

```
Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: 3e:62:29:ac:60:ce (3e:62:29:ac:60:ce), Dst: 9e:6a:95:21:5e:c0 (9e:6a:95:21:5e:c0)
Internet Protocol Version 4, Src:                    , Dst:
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 84
    Identification: 0x0000 (0)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xb755 [correct]
    Source:
    Destination:
Internet Control Message Protocol
    Type: 8
    Code: 0
```

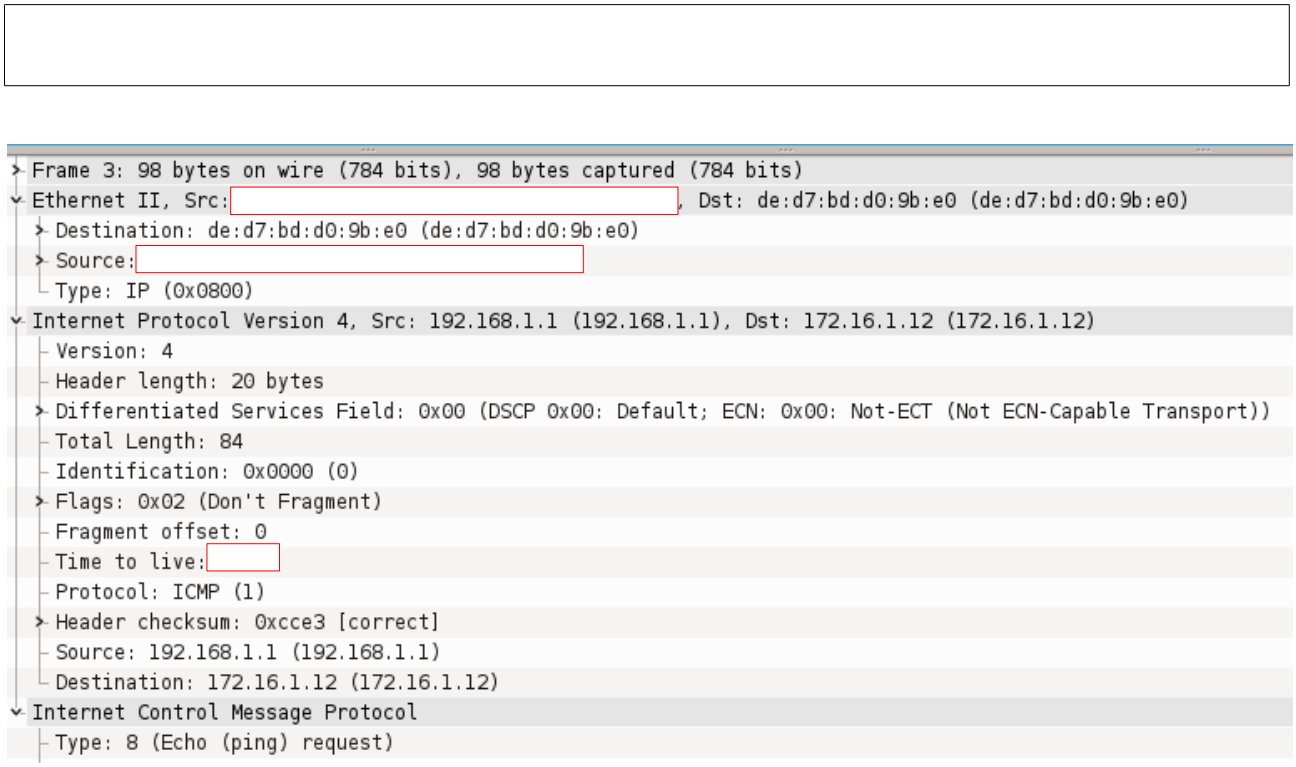
Commande utilisée :

2. Complétez le message ci-dessous.

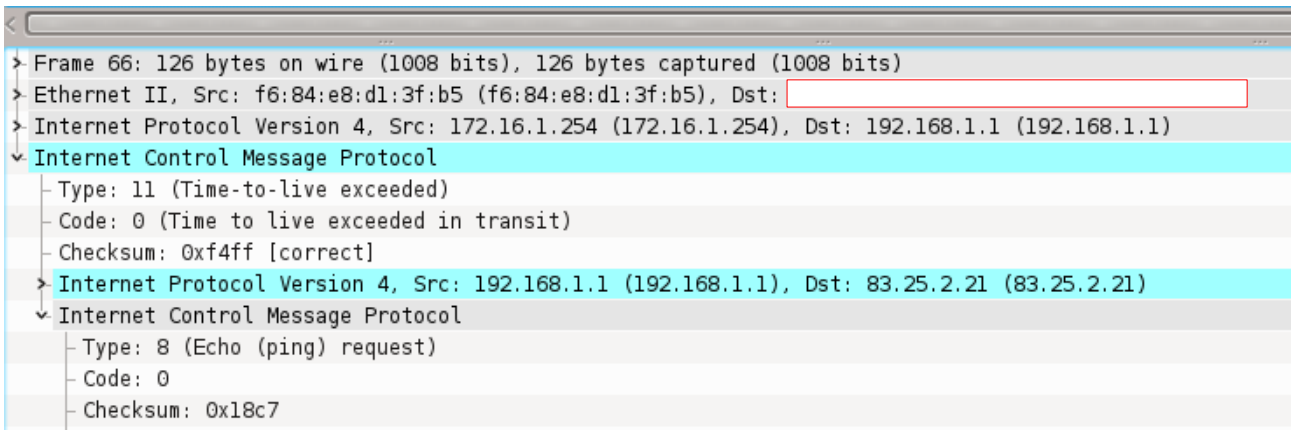


3. Complétez le message, et indiquez quelle commande a été utilisée (préciser la machine).

Commande utilisée :



4. Complétez le message et indiquez ce qui a dû se produire.



Explication :

2.2. Analyse de trame

Votre machine vient de recevoir le paquet suivant. Analysez-le pour en extraire les informations demandées. Vous pouvez vous aider du format du *IP header* rappelé ci-dessous :

32 bits			
Version (4 bits)	Longueur d'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)
Identification (16 bits)		Drapeau (3 bits)	Décalage fragment (13 bits)
Durée de vie (8 bits)	Protocole (8 bits)	Somme de contrôle en-tête (16 bits)	
Adresse IP source (32 bits)			
Adresse IP destination (32 bits)			
Données			

```
00 0c 29 97 68 42 f4 6d    04 1f 31 ad 08 00 45 00
00 54 0c fa 40 00 40 01    ab cf c0 a8 00 79 c0 a8
00 16 08 00 79 4a 0d 2e    00 01 00 ce 2b 55 00 00
00 00 7f 90 07 00 00 00    00 00 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d    1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d    2e 2f 30 31 32 33 34 35
36 37
```

1. Relevez les adresses des machines concernées par ce message

- l'adresse IP et l'adresse MAC de la machine « source »

  IP : _____ MAC : _____

- l'adresse IP et l'adresse MAC de la machine «destination»

  IP : _____ MAC : _____

2. Quel est le protocole de plus haut niveau ? Comment est-il encapsulé ?

3. Donnez le type de message avec le plus de détail possible

4. Donnez la commande qui a généré ce message

3. Connexions - Netstat

Identifiez à partir de l'affichage ci-dessous, obtenu sur la machine sur laquelle vous travaillez, les différents services proposés, ainsi que les différents clients connectés. Représentez l'ensemble de ces connexions via un schéma.

```
Local Address         Foreign Address       state
tcp   0 0.0.:21             0.0.0.0:*             LISTEN
tcp   :::23                 :::*                  LISTEN
tcp   192.168.102.1:335     213.34.21.38:44458    TIME_WAIT
tcp   :::335                :::*                  LISTEN
tcp   192.168.102.1:21      192.168.102.18:23422  ESTABLISHED
tcp   192.168.102.1:23      182.45.47.25:24522    TIME_WAIT
tcp   192.168.102.1:23      192.168.102.34:27882  ESTABLISHED
tcp   127.0.0.1:21          127.0.0.1:12762       ESTABLISHED
tcp   127.0.0.1:12762       127.0.0.1:21          ESTABLISHED
tcp   192.168.102.1:3542    172.16.5.254:22       ESTABLISHED
```

CONFIGURATION IP

1. Commandes client

1.1. Configuration réseau permanente

Dans le cas où on utilise une distribution *Debian* et le service *networking*, on peut utiliser la commande `ifconfig`, ou bien définir de manière « permanente » la configuration réseau. Dans ce cas, le fichier à utiliser est ***/etc/network/interfaces***. On va y définir, pour chaque interface réseau, la méthode d'attribution de l'adresse IP (statique ou dynamique), ainsi que les paramètres associés.

Exemple de fichier `interfaces`

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.56.11
netmask 255.255.255.0
gateway 192.168.56.1

auto eth1
iface eth1 inet dhcp
```

La machine décrite dans ce fichier possède une interface de ***loopback***, une interface ***`eth0`*** configurée manuellement, et une interface ***`eth1`*** configurée via DHCP.

Les modifications effectuées dans ce fichier ne seront prises en compte qu'au redémarrage de la machine. Afin que les modifications soient prises en compte immédiatement, on peut utiliser la commande suivante :

```
$ ifup eth0
```

L'autre possibilité est de forcer le redémarrage du service :

```
$ /etc/init.d/networking restart
```

1.2. La commande `traceroute`

La commande `traceroute` est une variante de la commande `ping` vue la semaine dernière. Elle permet non seulement de vérifier la connectivité avec un hôte donné, mais également de connaître le « chemin » emprunté par les paquets.

```
[redacted] ~ $ traceroute www.google.fr
traceroute to www.google.fr (216.58.211.67), 30 hops max, 60 byte packets
 1  ntp.iut.unilim.fr (192.168.0.254)  0.160 ms  0.155 ms  0.161 ms
 2  routeur-iut-info.iut.unilim.fr (164.81.20.254)  1.838 ms  2.532 ms  3.296 ms
 3  c6506-cr-relier.relier.fr (193.50.172.69)  4.589 ms  5.204 ms  6.088 ms
 4  193.51.189.74 (193.51.189.74)  9.623 ms  9.997 ms  10.150 ms
 5  po7-0-0-clermont-rtr-021.noc.renater.fr (193.51.177.132)  20.242 ms  20.853 ms  21.910 ms
 6  te0-6-0-1-lyon1-rtr-001.noc.renater.fr (193.51.177.148)  23.781 ms  23.103 ms  27.092 ms
 7  te1-1-lyon2-rtr-021.noc.renater.fr (193.51.177.166)  19.518 ms  39.457 ms  39.438 ms
 8  * * *
 9  72.14.223.254 (72.14.223.254)  25.394 ms  22.852 ms  23.457 ms
10  209.85.252.36 (209.85.252.36)  120.144 ms 209.85.252.194 (209.85.252.194)  15.930 ms 209.85
11  216.239.43.42 (216.239.43.42)  33.905 ms 216.239.43.68 (216.239.43.68)  24.844 ms 216.239.4
12  209.85.245.82 (209.85.245.82)  23.452 ms  19.772 ms  32.234 ms
13  72.14.233.81 (72.14.233.81)  28.950 ms  29.892 ms  27.021 ms
14  par03s14-in-f3.1e100.net (216.58.211.67)  25.392 ms  26.027 ms  22.408 ms
```

2. Serveur DHCP

2.1. Principe du DHCP

Attribution Dynamique

La machine cliente n'ayant pas d'@IP fixe, elle va demander à un serveur DHCP de lui en «prêter» une. Le serveur DHCP pourra fournir aux clients d'autres informations réseaux telles que :

- Valeur du netmask
- Nom de domaine
- Nom ou @IP du ou des serveurs de domaines
- Nom ou @IP de la passerelle.

Remarque : Sur un réseau, on mélange adressage statique et adressage dynamique. Certaines machines ont une @IP fixée une fois pour toutes, d'autres ont une @IP dynamique. Les serveurs de noms, la passerelle, le serveur DHCP, certaines imprimantes ont généralement une @IP statique.

Avantage : DHCP facilite la gestion des @IP.

- Travail fastidieux, non paramétrable et source d'erreurs
- Optimise l'utilisation des @IP

Exemple : connexion à Internet via un fournisseur d'accès. Il fournit automatiquement à votre PC une adresse IP pour l'accès réseau à distance. Cette adresse sera bloquée durant votre session et redeviendra disponible lors de la fermeture de la session. Le serveur DHCP pourra attribuer à un nouveau client cette adresse redevenue « libre »

Inconvénients de DHCP

On a vu que DHCP offre une souplesse quant à l'administration des postes clients, et peut gérer la pénurie d'@IP. Si un poste client n'a pas d'@IP, il la demande au serveur DHCP. Une solution centralisée présente néanmoins également des désavantages :

- Que se passe-t-il si le serveur DHCP est en panne ?
  Une solution est d'avoir 2 serveurs DHCP – mais attention à la configuration

- Interférence entre les DHCP

  L'utilisation non souhaitée de plusieurs serveurs DHCP sur un même réseau va très vite conduire à des conflits d'IP et à la paralysie du réseau.

2.2. Mode d'attribution par un DHCP

Un serveur DHCP propose 2 façons d'attribuer des @IP dynamiques.

- Une attribution fixe – on dit encore « manuelle »
- Une attribution changeante – on dit encore « dynamique »

Attribution fixe

Dans ce cas, un serveur DHCP attribuera toujours la même adresse au demandeur, et cette adresse ne sera jamais proposée à une autre machine. Ceci est utile pour les machines particulières (passerelle, imprimante, serveur, etc. …). On peut également utiliser ce principe de fonctionnement pour des raisons de « sécurité » (filtrage des clients).

Attribution changeante (dynamique)

Dans ce cas de figure qui est le plus répandu, lorsqu'une machine fait une demande d'adresse, le serveur DHCP lui proposera une IP disponible, située dans une plage prédéfinie. Lors d'une demande ulterieure, une même machine est susceptible d'obtenir une adresse différente.

Notion de bail (lease)

Dans les deux cas, une adresse n'est pas « donnée », mais « prêtée » pour une durée fixée, qui est déterminée par le serveur. On dit que ce dernier attribue un bail pour une machine, qui doit être renouvelé avant expiration si la machine cliente veut conserver son adresse IP.

L'ensemble de ces baux est conservé dans un fichier qui est actualisé en permanence, on le trouve généralement dans le dossier */var/dhcp* :

```
lease 192.168.1.11 {
  starts 3 2012/10/24 08:53:10;
  ends 3 2012/10/24 09:03:10;
  cltt 3 2012/10/24 08:53:10;
  binding state active;
  next binding state free;
  hardware ethernet 2e:18:cc:d4:8c:e7;
}
lease 192.168.1.10 {
  starts 3 2012/10/24 08:53:53;
```

3. Configuration d'un DHCP sous Linux

3.1. Installation/démarrage

Il existe de multiples versions du serveur DHCP (y compris pour une même distribution). Lors des TP, vous utiliserez la version fournie par le paquet ***isc-dhcp-server*** qui devra être installé de la manière suivante :

```
$ apt-get install isc-dhcp-server
```

Une fois le serveur installé, il sera contrôlé via le script correspondant, comme pour tout serveur sous Linux :

- `service isc-dhcp-server` **`start`** pour le démarrer,
- `service isc-dhcp-server` **`stop`** pour l'arrêter,
- `service isc-dhcp-server` **`restart`** pour le redémarrer.

En plus de ces commandes, on peut également utiliser la commande `dhcpd -t`, qui va permettre de vérifier la syntaxe du fichier de configuration sans démarrer le serveur.

3.2. Configuration

La configuration du serveur sera contenue dans le fichier ***/etc/dhcp/dhcpd.conf***, mais cet emplacement peut différer pour une autre distribution ou une autre version du serveur. Il s'agit d'un fichier texte contenant un certain nombre de directives et les valeurs associées, les plus communes étant présentées ci-dessous.

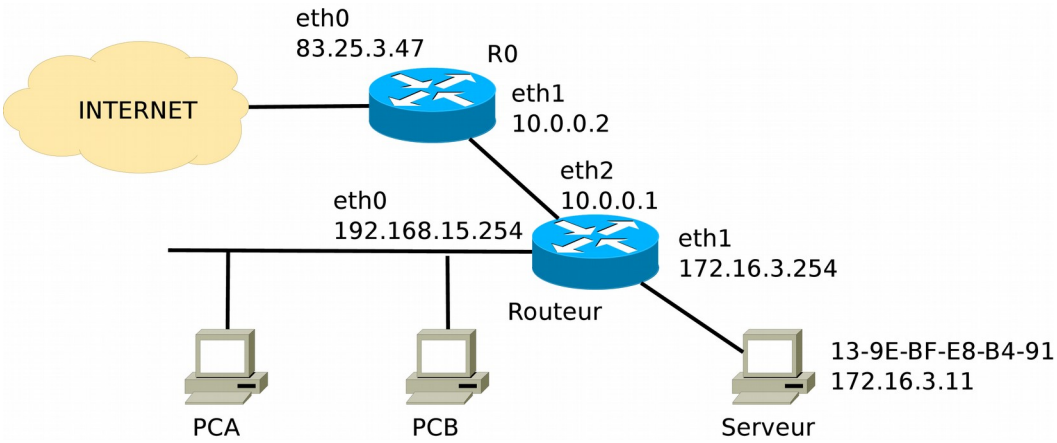
Exemple simple de fichier *dhcpd.conf*

```
ddns-update-style none;

subnet 137.12.84.0 netmask 255.255.255.0
{
     range 137.12.84.15  137.12.84.254;
     default-lease-time 21600;
     max-lease-time 43200;
     option routers 137.12.84.10;
     option domain-name "domain.fr";
     option domain-name-servers 137.12.84.11;
}

host pc1 {
     hardware ethernet 00:4A:5C:24:3E:FF;
     fixed-address 137.12.84.20;
}
```

- subnet :
- range :
- option routers :
- option domain-name :
- option domain-name-servers :
- host :
- hardware ethernet :
- fixed-address :

4. Exercice

Pour tout l'exercice, on considère le réseau ci-dessous :



1. Donnez la commande permettant d'affecter son adresse IP à l'interface ***eth1*** de **R0**.

Commande

2. Donnez le contenu du fichier */etc/network/interfaces* de la machine **Routeur**.

Fichier */etc/network/interfaces* de **Routeur**

3. Donnez le contenu du fichier *dhcpd.conf*, sachant que le serveur sera situé sur la machine **Routeur**, et qu'il devra délivrer les adresses pour le sous-réseau des PC et pour celui des serveurs. La plage d'adresse 101-200 sera utilisée pour les 2 réseaux.

Fichier *dhcpd.conf*

4. Quelle modification faut-il apporter à ce fichier pour que la machine **Serveur** reçoive 172.16.3.11 comme adresse IP fixe ?

Modification de *dhcpd.conf*