

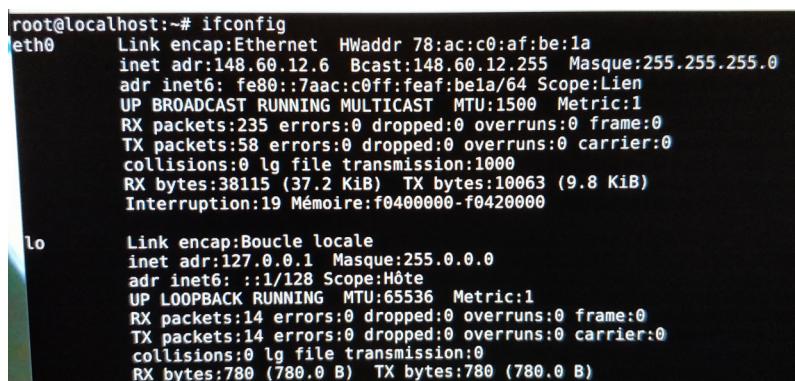
PRIEUR Fanny
DEROCLES Manon
M1 SSR

RPS TP2

ETUDE DE PROTOCOLES DE L'INTERNET

Manip 1 : Découverte préliminaire de la salle I207 de tp de réseaux et aspects d'Ethernet et d'IP (adressage et routage)

Question 1.1) Avec la commande **ifconfig** nous obtenons notre adresse IP : **148.60.12.6**
Avec la commande **hostname** nous obtenons le nom de notre machine : **localhost**



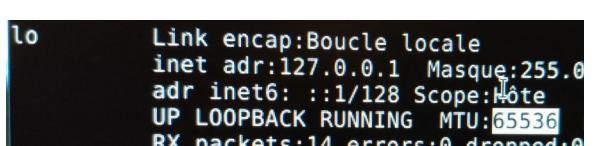
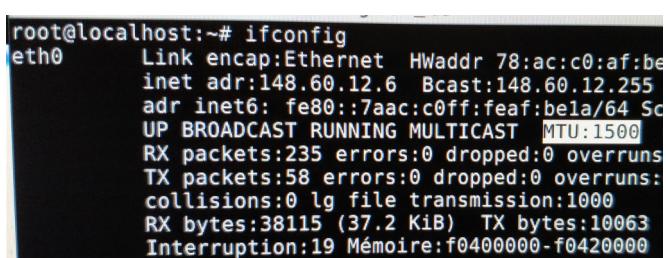
```
root@localhost:~# ifconfig
eth0      Link encap:Ethernet HWaddr 78:ac:c0:af:be:1a
          inet adr:148.60.12.6 Bcast:148.60.12.255 Masque:255.255.255.0
          adr inet6: fe80::7aac:c0ff:feaf:bela/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:235 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:38115 (37.2 KiB) TX bytes:10063 (9.8 KiB)
          Interruption:19 Mémoire:f0400000-f0420000

lo        Link encap:Boucle locale
          inet adr:127.0.0.1 Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:780 (780.0 B) TX bytes:780 (780.0 B)
```



```
root@localhost:~# hostname
localhost
```

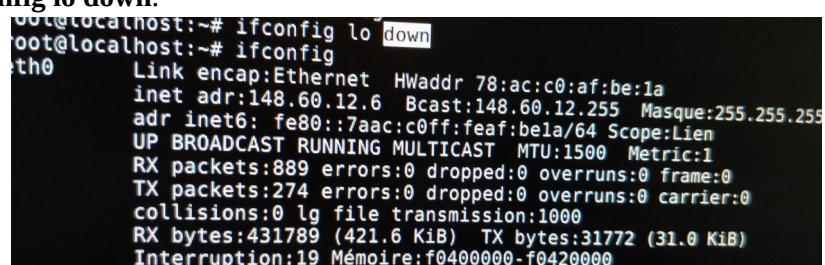
Question 1.2) En utilisant **ifconfig** nous comptons 2 interfaces Ethernet utilisé par notre machine.
-**eth0** qui possède un **MTU=1500**
-**lo** qui possède un **MTU=65536**



```
root@localhost:~# ifconfig
eth0      Link encap:Ethernet HWaddr 78:ac:c0:af:be:1a
          inet adr:148.60.12.6 Bcast:148.60.12.255 Masque:255.255.255.0
          adr inet6: fe80::7aac:c0ff:feaf:bela/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:235 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:38115 (37.2 KiB) TX bytes:10063 (9.8 KiB)
          Interruption:19 Mémoire:f0400000-f0420000

lo        Link encap:Boucle locale
          inet adr:127.0.0.1 Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:780 (780.0 B) TX bytes:780 (780.0 B)
```

Question 1.3) Pour désactiver l'interface **lo** afin de conserver l'interface **eth0** nous utilisons la commande **ifconfig lo down**.



```
root@localhost:~# ifconfig lo down
root@localhost:~# ifconfig
eth0      Link encap:Ethernet HWaddr 78:ac:c0:af:be:1a
          inet adr:148.60.12.6 Bcast:148.60.12.255 Masque:255.255.255.0
          adr inet6: fe80::7aac:c0ff:feaf:bela/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:889 errors:0 dropped:0 overruns:0 frame:0
          TX packets:274 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:431789 (421.6 KiB) TX bytes:31772 (31.0 KiB)
          Interruption:19 Mémoire:f0400000-f0420000
```

PRIEUR Fanny
DEROCLES Manon
M1 SSR

RPS TP2

ETUDE DE PROTOCOLES DE L'INTERNET

Question 1.4) La route par défaut n'a pas la bonne adresse.

Pour ajouter la bonne route par défaut vers le routeur il nous faut taper :

route add default gw 148.60.12.254 netmask 255.255.255.0 dev eth0

Puis nous vérifions que la route a bien été créée avec **nslookup 148.60.12.254**.

La route par défaut indiquera comment s'achemine le traffic qui ne correspond à aucune entrée dans la table de routage. Nous faisons **nslookup** afin de vérifier que la route a bien été créée avec la bonne adresse car sur la capture l'adresse IP n'est pas affiché.

```
root@localhost:~# route add default gw 148.60.12.254 netmask 255.255.255.0 dev eth0
IOCADDRT: Le fichier existe
root@localhost:~# route
table de routage IP du noyau
destination      Passerelle      Genmask        Indic Metric Ref    Use Iface
default          vlan12-gw.istic 255.255.255.0  UG    0      0      0 eth0
default          vlan12-gw.istic 0.0.0.0       UG    0      0      0 eth0
default          *              255.255.255.0   U     0      0      0 eth0
148.60.12.0      *
root@localhost:~# nslookup 148.60.12.254
Server:          148.60.4.1
Address:         148.60.4.1#53
254.12.60.148.in-addr.arpa  name = vlan12-gw.istic.univ-rennes1.fr.
```

**PRIEUR Fanny
DEROCLES Manon
M1 SSR**

RPS TP2

ETUDE DE PROTOCOLES DE L'INTERNET

Manip 2 : Analyse des protocoles ARP et ICMP.

Question 2.1) ARP est un protocole de resolution d'adresse. A partir d'une adresse IP il peut déterminer une adresse MAC. Pour vider la table (cache) ARP de notre machine : **arp -d @ip**

```
ost:~# arp -d 148.60.12.253  
ost:~# arp -d 148.60.12.254
```

Question 2.2) Pour envoyer un ping vers la machine `anubis.ifsic.univ-rennes1.fr` en ne générant qu'un seul paquet nous entrons : **ping -c 1 anubis.ifsic.univ-rennes1.fr**

```
root@localhost:~# ping -c 1 anubis.ifsic.univ-rennes1.fr
PING anubis.ifsic.univ-rennes1.fr (148.60.12.25) 56(84) bytes of data.
64 bytes from anubis.istic.univ-rennes1.fr (148.60.12.25): icmp_seq=1 ttl=64 time=0.000 ms
--- anubis.ifsic.univ-rennes1.fr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.214/0.214/0.214/0.000 ms
root@localhost:~#
```

Filter:	arp icmp	Expression...		Clear	Apply	Enregistrer	Filter
No.	Time	Source	Destination	Protocol	Length	Info	
32	2.002514000	Cisco_0e:f6:6f	Broadcast	ARP	60	Who has 148.60.12.137? Tell 148.60.12.254	
39	5.243063000	Cisco_0e:f6:6f	Broadcast	ARP	60	Who has 148.60.12.27? Tell 148.60.12.254	
52	7.776193000	Dell_9e:11:1c	Broadcast	ARP	60	Who has 148.60.12.254? Tell 148.60.12.253	
62	9.453896000	148.60.12.6	148.60.12.25	ICMP	98	Echo (ping) request id=0x088a, seq=1/256, ttl=64 (reply in 63)	
63	9.454098000	148.60.12.25	148.60.12.6	ICMP	98	Echo (ping) reply id=0x088a, seq=1/256, ttl=64 (request in 62)	

Question 2.3) Voici les différents champs principaux d'un message ARP

Hardware Type : Indique le format de l'entête ARP

Protocol Type : Indique le type de protocole couche 3 qu'il utilise ARP. Ici c'est IP.

Hardware Size : Correspond à la longueur de l'adresse physique (MAC) soit 6 octets.

Protocol Size : Correspond à l'adresse réseaux (IP) soit 4 octets.

Opcode: Permet de connaître la fonction du message.
Ici c'est une requête.

Sender MAC address : Indique l'adresse MAC de l'émetteur (source).

Sender MAC address : Indique l'adresse MAC de l'émetteur (source)

Target MAC address : Adresse MAC du destinataire. Le champs est à 0 car on ne connaît pas encore cette adresse.

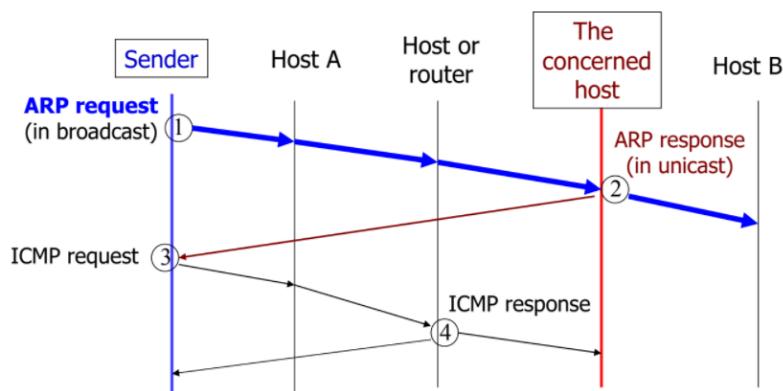
Target IP address : Indique l'adresse IP du destinataire

```
.... .0 .... . . . . = IG bit: individual addr  
Type: ARP (0x0806)  
Padding: 00000000000000000000000000000000  
Address Resolution Protocol (request)   
Hardware type: Ethernet (1)  
Protocol type: IP (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: request (1)  
Sender MAC address: Dell_9e:11:1c (d4:ae:52:9e:11:1c)  
Sender IP address: 148.60.12.253 (148.60.12.253)  
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)  
Target IP address: 148.60.12.254 (148.60.12.254)
```

RPS TP2

ETUDE DE PROTOCOLES DE L'INTERNET

Question 2.4)



ARP envoie en broadcast à toutes les machines puis la machine concerné répond en unicast en ICMP.

Question 2.5) Voici les différents champs principaux d'un message ICMP

ICMP permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs mais d'en informer le différents émetteurs des datagrammes.

Type et code : Représentent la définition de message d'erreur contenu. Les deux étant à 0, cela signifie que c'est la réponse à une demande d'écho.

Checksum : Représente la validité du paquet de la couche 3. Ici il n'a pas eu de problème.

Identifier : Identifiant de l'émetteur.

Sequence number : Permet au récepteur d'identifier si il manque un paquet.

```
[Internet Control Message Protocol]
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x386a [correct]
Identifier (BE): 2186 (0x088a)
Identifier (LE): 35336 (0x8a08)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Request frame: 62]
[Response time: 0,202 ms]
Timestamp from icmp data: Oct 13, 2017 09:13:40.000000000 CEST
[Timestamp from icmp data (relative): 0.816965000 seconds]
```

PRIEUR Fanny
DEROCLES Manon
M1 SSR

RPS TP2

ETUDE DE PROTOCOLES DE L'INTERNET

Question 2.6) Lorsque nous comparons l' ICMP Request de l'ICMP Reply nous pouvons constater que le checksum est different. Sachant que le protocole ICMP correspond à de la détection d'erreur durant les échanges de datagrammes sur Internet, alors ici l'échange s'est bien passé.

```
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x306a [correct]
Identifier (BE): 2186 (0x088a)
Identifier (LE): 35336 (0x8a08)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Response frame: 63]
Timestamp from icmp data: Oct 13, 2017 09:13:40.000000000 CEST
[Timestamp from icmp data (relative): 0.816763000 seconds]
```

```
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x386a [correct]
Identifier (BE): 2186 (0x088a)
Identifier (LE): 35336 (0x8a08)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Request frame: 62]
[Response time: 0,202 ms]
Timestamp from icmp data: Oct 13, 2017 09:13:40.000000000 CEST
[Timestamp from icmp data (relative): 0.816965000 seconds]
```

PRIEUR Fanny
DEROCLES Manon
M1 SSR

RPS TP2

ETUDE DE PROTOCOLES DE L'INTERNET

Manip 3 : Etude de la fragmentation IP.

Question 3.1) Pour envoyer un ping vers la machine 148.60.4.10 avec une taille de données de 2000octets nous tapons dans le terminal : **ping -s 2000 148.60.4.10**

Le premier fragment du paquet IP est identifié grâce au numéro. Ici numéro #24 et #25. Dans l'encapsulation on voit que c'est de type ethernet et grace au champs **ipv4 fragment**. Il y en a deux #24 et #25 dans le champs **Fragment count**. Le premier #24 étant de 0 a 1479 et l'autre #25 de 1480 a 2007. La longueur de ce paquet IP est de 2008 octets.

```
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 548
Identification: 0x4e0b (19979)
Flags: 0x00
Fragment offset: 1480
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0xf18c [validation disabled]
Source: 148.60.12.6 (148.60.12.6)
Destination: 148.60.4.10 (148.60.4.10)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
[2 IPv4 Fragments (2008 bytes): #24(1480), #25(528)]
[Frame: 24, payload: 0-1479 (1480 bytes)]
[Frame: 25, payload: 1480-2007 (528 bytes)]
[Fragment count: 2]
[Reassembled IPv4 length: 2008]
[Reassembled IPv4 data: 080052ed092200012071e05900000000803c0f00000000...]
Internet Control Message Protocol
```

Question 3.2) Le deuxième fragment du paquet IP est identifié grâce au numéro. Ici numéro #26 et #27. Dans l'encapsulation on voit que c'est de type ethernet et grace au champs **ipv4 fragment**. Il y en a deux #26 et #27 dans le champs **Fragment count**. Le premier #26 étant de 0 a 1479 et l'autre #27 de 1480 a 2007. La longueur de ce paquet IP est de 2008 octets. Non il ni a pas d'autres paquets qui suivent.

```
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 548
Identification: 0xc3c9 (50121)
Flags: 0x00
Fragment offset: 1480
Time to live: 63
Protocol: ICMP (1)
Header checksum: 0x7cce [validation disabled]
Source: 148.60.4.10 (148.60.4.10)
Destination: 148.60.12.6 (148.60.12.6)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
[2 IPv4 Fragments (2008 bytes): #26(1480), #27(528)]
[Frame: 26, payload: 0-1479 (1480 bytes)]
[Frame: 27, payload: 1480-2007 (528 bytes)]
[Fragment count: 2]
[Reassembled IPv4 length: 2008]
[Reassembled IPv4 data: 00005aed092200012071e05900000000803c0f00000000...]
```

Question 3.3) Les champs qui diffèrent entre les deux paquets sont l'offset et la taille.