

COMPTE RENDU TP1 RSP

Partie 1 : Interrogations d'une infrastructure de réseau

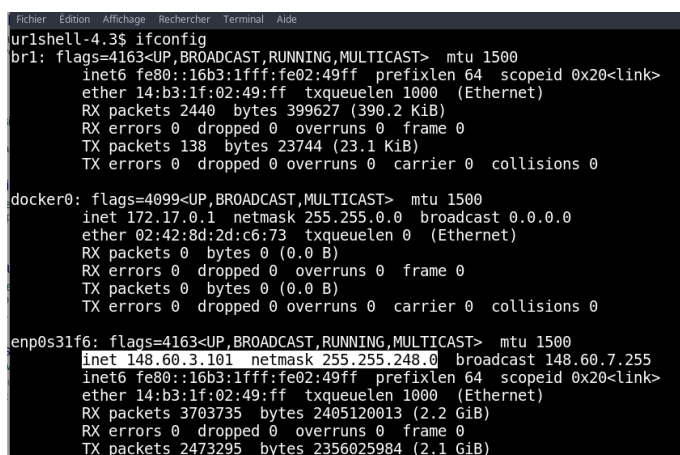
Question 1 :

La commande utilisé est : **ifconfig**

Adresse IP : **148.60.3.101**

Masque de Sous-réseaux : **255.255.248.0**

Pour le nom de la machine on tape la commande hostname : **e008m5**



```
Fichier Edition Affichage Rechercher Terminal Aide
ur1shell-4.3$ ifconfig
br1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::16b3:1fff:fe02:49ff prefixlen 64 scopeid 0x20<link>
    ether 14:b3:1f:02:49:ff txqueuelen 1000 (Ethernet)
    RX packets 2440 bytes 399627 (390.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 138 bytes 23744 (23.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 0.0.0.0
    ether 02:42:8d:2d:c6:73 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 148.60.3.101 netmask 255.255.248.0 broadcast 148.60.7.255
    inet6 fe80::16b3:1fff:fe02:49ff prefixlen 64 scopeid 0x20<link>
    ether 14:b3:1f:02:49:ff txqueuelen 1000 (Ethernet)
    RX packets 3703735 bytes 2405120013 (2.2 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2473295 bytes 2356025984 (2.1 GiB)
```

Question 2 :

La commande **ifconfig** permet également de trouver le protocole utilisé à la couche liaison de donnée qui est le protocole Ethernet. Il y a aussi l'adresse Mac qui est présente et les informations de la question 1.

Question 3 :

Notre adresse IP est 148.60.3.101. Pour déterminer la classe de notre adresse IP on décompte 148 en binaire. Cela donne **1001 1000**. Qui donne la classe B. On a donc 14 bits pour le sous-réseaux et 16 bits pour les hôtes.

Quand on fait un masquage entre l'adresse IP et le masque de sous-réseaux on obtiens l'adresse **148.60.0.0** qui nous permet d'allouer des adresses IP pour ce sous réseaux.

On a donc un adressage possible d'adresses de **148.60.0.0** à **148.60.255.255**.

On ne peut théoriquement pas connaître le plan d'adressage des autres bâtiments sans leurs adresses de sous réseaux. On peut aussi taper **netstat -route** pour avoir l'adresse directement.

Question 4 :

Pour savoir le nom de la machine la commande est **traceroute <@ip>**.

L'adresse IP 148.60.10.15 n'est pas active car en pingant cette adresse tout les paquets sont perdu et la machine ne nous envoie aucune réponse. La machine 148.60.4.3 a la statut indéterminée car il y a des erreurs qui se produise pendant le ping. Elle pourrait être active donc le fait qu'elle perde tout les paquets ne veut pas dire qu'elle n'est pas active.

COMPTE RENDU TP1 RSP

Les machines 148.60.12.7 et 148.60.2.200 et 148.60.1.39 existe car ça pingue bien.

Le nom de 148.60.12.7 est **i207m07**

le nom de 148.60.2.200 est **e212m08**

le nom de 148.60.1.39 est **d022m07**

Question 5 :

Http port 80

Ftp port 20 pour le flux de données et 21 pour le flux de contrôle pour le transfert de fichiers

Telnet port 23

Smtp port 25

Ssh port 22

Pour afficher les différents port il faudrait que nous soyons administrateur afin d'utiliser la commande **nmap -sS -sU -sV 148.60.3.101**

Question 6 :

La commande a utilise est **netstat -natp**

Les sessions Internet principales en cours correspondent aux connexions distantes (page web, ssh, ping etc..) utilisé avec notre adresse IP.

```
Fichier  Édition  Affichage  Recherche  Terminal  Aide
Address: 195.238.226.27

urlshell-4.3$ netstat -natp
(Tous les processus ne peuvent être identifiés, les infos sur les processus
non possédés ne seront pas affichées, vous devez être root pour les voir toutes.)
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat PID/Progr
tcp 0 0 0 127.0.0.1:40327 0.0.0.0:* LISTEN -
tcp 0 0 0 127.0.0.1:9000 0.0.0.0:* LISTEN -
tcp 0 0 0 0.0.0.0:50090 0.0.0.0:* LISTEN -
tcp 0 0 0 0.0.0.0:42127 0.0.0.0:* LISTEN -
tcp 0 0 0 0.0.0.0:111 0.0.0.0:* LISTEN -
tcp 0 0 0 0.0.0.0:50070 0.0.0.0:* LISTEN -
tcp 0 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp 0 0 0 0.0.0.0:50010 0.0.0.0:* LISTEN -
tcp 0 0 0 0.0.0.0:50075 0.0.0.0:* LISTEN -
tcp 0 0 0 0.0.0.0:50020 0.0.0.0:* LISTEN -
tcp 0 0 0 148.60.3.101:37584 129.20.123.1:636 ESTABLISHED -
tcp 0 0 0 148.60.3.101:50120 52.236.33.247:443 ESTABLISHED 12924/fi
tcp 0 0 0 148.60.3.101:895 148.60.15.116:2049 ESTABLISHED -
tcp 0 0 0 148.60.3.101:37586 129.20.123.1:636 ESTABLISHED -
tcp 0 0 0 148.60.3.101:782 129.20.128.182:2049 ESTABLISHED -
tcp 1 0 0 148.60.3.101:43914 148.60.15.102:631 CLOSE WAIT 12465/ci
tcp 0 0 0 127.0.0.1:60436 127.0.0.1:9000 TIME WAIT -
tcp 0 0 0 148.60.3.101:822 148.60.15.129:2049 ESTABLISHED -
tcp 0 0 0 148.60.3.101:36726 13.107.42.11:443 ESTABLISHED 12924/fi
tcp 0 0 0 127.0.0.1:9000 127.0.0.1:60438 ESTABLISHED -
tcp 0 0 0 127.0.0.1:49162 127.0.0.1:9000 ESTABLISHED -
tcp 0 0 0 127.0.0.1:60438 127.0.0.1:9000 ESTABLISHED -
tcp 0 0 0 127.0.0.1:9000 127.0.0.1:49162 ESTABLISHED -
tcp 0 0 0 148.60.3.101:59642 40.77.226.194:443 ESTABLISHED 12924/fi
tcp6 0 0 0 :::8040 :::* LISTEN -
tcp6 0 0 0 :::8042 :::* LISTEN -
tcp6 0 0 0 :::111 :::* LISTEN -
tcp6 0 0 0 :::44819 :::* LISTEN -
tcp6 0 0 0 :::22 :::* LISTEN -
tcp6 0 0 0 :::8088 :::* LISTEN -
tcp6 0 0 0 :::34777 :::* LISTEN -
tcp6 0 0 0 :::8030 :::* LISTEN -
tcp6 0 0 0 :::8031 :::* LISTEN -
tcp6 0 0 0 :::8032 :::* LISTEN -
tcp6 0 0 0 :::8033 :::* LISTEN -
tcp6 0 0 0 148.60.3.101:33244 148.60.3.101:8031 ESTABLISHED -
tcp6 0 0 0 148.60.3.101:8031 148.60.3.101:33244 ESTABLISHED -
urlshell-4.3$
```

COMPTE RENDU TP1 RSP

Question 7 :

Pour afficher la table de routage il faut utiliser la commande **route -n**

```

Fichier  Édition  Affichage  Rechercher  Terminal  Aide
urlshell-4.3$ route -n
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref       Use Iface
0.0.0.0          148.60.7.254    0.0.0.0          UG        100    0        0 enp0s31f6
148.60.0.0       0.0.0.0         255.255.248.0    U        100    0        0 enp0s31f6
169.254.0.0      0.0.0.0         255.255.0.0      U       1004    0        0 br1
172.17.0.0       0.0.0.0         255.255.0.0      U         0    0        0 docker0
urlshell-4.3$ |
  
```

Question 8 :

On utilise **nslookup <adresse>** afin de connaître les serveurs DNS.

Machines/Service	DNS
Notre machine :148.60.3.101	148.60.4.1
yasuragi.irisa.fr	Non déterminé
www.google.fr	216.58.211.163
www.tahi.org	203.178.141.201
www.etsi.org	198.238.226.27
www.mit.edu	104.96.16.12

```

urlshell-4.3$ nslookup yasuragi.irisa.fr
Server:      148.60.4.1
Address:     148.60.4.1#53

** server can't find yasuragi.irisa.fr: NXDOMAIN

urlshell-4.3$ nslookup www.google.fr
Server:      148.60.4.1
Address:     148.60.4.1#53

Non-authoritative answer:
Name:   www.google.fr
Address: 216.58.211.163

urlshell-4.3$
urlshell-4.3$
urlshell-4.3$ nslookup www.mit.edu
Server:      148.60.4.1
Address:     148.60.4.1#53

Non-authoritative answer:
www.mit.edu canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.96.16.12
  
```

```

urlshell-4.3$ nslookup www.tahi.org
Server:      148.60.4.1
Address:     148.60.4.1#53

Non-authoritative answer:
Name:   www.tahi.org
Address: 203.178.141.201

urlshell-4.3$ nslookup etsi.org
Server:      148.60.4.1
Address:     148.60.4.1#53

Non-authoritative answer:
Name:   etsi.org
Address: 195.238.226.27
  
```

```

Fichier  Édition  Affichage  Rechercher  Terminal  Aide
urlshell-4.3$ nslookup 148.60.3.101
Server:      148.60.4.1
Address:     148.60.4.1#53

101.3.60.148.in-addr.arpa      name = e008m05.istic.univ-rennes1.fr.
  
```

COMPTE RENDU TP1 RSP

Question 9 :

Pour connaître le chemin suivi par les paquets pour atteindre les machines/services on utilise la commande **dig** www.google.fr +trace.

```
urlshell-4.3$ dig www.google.fr +trace

;<> DiG 9.10.4-P8-RedHat-9.10.4-4.P8.fc25 <> www.google.fr +trace
;; global options: +cmd

501922 IN      NS      g.root-servers.net.
501922 IN      NS      i.root-servers.net.
501922 IN      NS      d.root-servers.net.
501922 IN      NS      a.root-servers.net.
501922 IN      NS      e.root-servers.net.
501922 IN      NS      l.root-servers.net.
501922 IN      NS      b.root-servers.net.
501922 IN      NS      f.root-servers.net.
501922 IN      NS      k.root-servers.net.
501922 IN      NS      c.root-servers.net.
501922 IN      NS      j.root-servers.net.
501922 IN      NS      h.root-servers.net.
501922 IN      NS      m.root-servers.net.
501922 IN      RRSIG   NS 8 0 518400 20171018170000 20171005160000 46809 . KL9N9hZL0+qAz3HTc+Vs9PY/BP+1at0Jvb+WF6MK9UzIGRa92Kbc1yMn 0qeRFkXIVG6KuKU0
EsCvUwPlD0/Ipd6ZiSYb0WodA5RV5xpLnk+/5v 41bnGquU7UHV4aMEMvNUc7HEp2BM7+tjsufZ9/AyUIbRitkh/SGIL4Km Za0GIA==
;; Received 1097 bytes from 148.60.4.1#53(148.60.4.1) in 0 ms

fr.          172800 IN      NS      d.nic.fr.
fr.          172800 IN      NS      g.ext.nic.fr.
fr.          172800 IN      NS      d.ext.nic.fr.
fr.          172800 IN      NS      f.ext.nic.fr.
fr.          172800 IN      NS      e.ext.nic.fr.
fr.          86400  IN      DS      35095 8 2 23C6CAADC9927EE98061F2B52C9B8DA6B53F3F648F814A4A86A0FAF9 843E2C4E
fr.          86400  IN      DS      9392 8 2 BAE7AB5D1604A18AB4DBDE018A3C12142E4EDBECE8AFC0E207901886 B2DD2292
fr.          86400  IN      RRSIG   DS 8 1 86400 20171019050000 20171006040000 46809 . cmRYB8mWqBPqJRg5g76i9x5bVmxq8S2hgRu9bf8UkLH2zGlqcoTdbJ/ wxDHZy9R0oZrGQze
5FHJ9j05e2cYPTTL2LnBu62q7+wi3sxcJbAeEPC wd6H3QkkqNB0+IVxTyYG7cQvL9fEDlGvoBqWYqFESN8YaFyK505B4YK zF6hh6ieuKbL/EIsEB6+eML6vaU+QzZRYTLX4gbp/UQfJ8CsJTTIdIq 5iHu13S42Z3Jau9LAYk
TP50Lr5GJPvIhw7AGooo/b4GjnUeyyFv01r7H yT4HNxdrTI4KxATPhSL/VLXLL4W2XI8qhovSBTCA+eHnRulP1CawnhgH jSL3HA==
;; Received 733 bytes from 199.7.91.13#53(d.root-servers.net) in 18 ms

google.fr.   172800 IN      NS      ns1.google.com.
google.fr.   172800 IN      NS      ns4.google.com.
google.fr.   172800 IN      NS      ns3.google.com.
google.fr.   172800 IN      NS      ns2.google.com.
EJ3N00DGNMIITGP0Q498J19P0FARJ2IO.fr. 5400 IN NSEC3 1 1 1 892E8109 EJ3N5GB1DPP21CINGB0FU7A3UQ7IPKHL NS SOA TXT NAPTR RRSIG DNSKEY NSEC3PARAM
EJ3N00DGNMIITGP0Q498J19P0FARJ2IO.fr. 5400 IN RRSIG NSEC3 8 2 5400 20171204120019 20171005120019 409 fr. 08xg2s5G2MLSAJssKP7DQPP8S5MhF9m+okTUq+UoFgwsLR0c1x2F4zTf Y5xdw+NlrlJC
qQ5SXK9j0Yc21Rm0bXdkK44YrYrGY00d30PodyByr9gG Zx0qwniPI6QENUVstC0YgG0zqG0Azc9oeipW0wRkEu4eSej4BY+fuEBL 9Is=
BK5CBVS0HD0D3RG745FIBG573DHTCPTV.fr. 5400 IN NSEC3 1 1 1 892E8109 BK5FENENRF2BBCH4SS0TRBUf63HSDKB0 NS DS RRSIG
BK5CBVS0HD0D3RG745FIBG573DHTCPTV.fr. 5400 IN RRSIG NSEC3 8 2 5400 20171204120019 20171005120019 409 fr. 1qtZrsXlCFT39m0pQz7fPwJokaMD9jxosvHa6xnqZ+uzrf0YyuzCWlm 0au550KrIDj3
PpY+RosaXwXsefg50n72X/8Rh5me9doFdEBwXVB5Mnh Iqflh20K4I7Zrt04XXXIX2m000uJmwNPhu0LZyiwnapDVPmFP8Jcbao H5U=
;; Received 615 bytes from 192.5.4.2#53(d.ext.nic.fr) in 20 ms
```

Dans cet exemple nous suivons les paquets envoyé à Google. Ces paquets passent d'abord par les serveurs DNS **g,i,d,a,e,l,b,f,k,c,j,h,m** du réseau de l'istic appelé **root-servers.net**. Puis ils passent dans les serveurs DNS **d,g,d,f,e** de **nic.fr** pour le **d** et de **ext.nic.fr** pour les autres. Et enfin ils passent par les serveurs DNS **ns1,ns4,ns3,ns2** de **google.com**.

Sur le site ping.eu quand on utilise l'onglet **tracert** on remarque que les paquets ne prennent pas forcément la même route. C'est la même manipulation pour les autres machines/services.

COMPTE RENDU TP1 RSP

2-Analyse de traces Ethernet et IP avec Wireshark

Question 1 :

On retrouve bien notre adresse **IP 148.60.3.101** (machine perso pour finir le tp : **IP= 192.168.1.10** et **MAC=e0:94:67:54:0b:00**). C'est donc cohérent.

18	0.733004974	148.60.3.101	148.60.3.101	TCP	68	33244 → 8031 [ACK] Seq=198 Ack=44 Win=342 Len=0 TSval=3715090280 TSecr=3715090280
25	1.369240251	148.60.3.101	93.184.220.29	TCP	68	45768 → 80 [ACK] Seq=1 Ack=1 Win=266 Len=0 TSval=2655058786 TSecr=1363642612
26	1.369247595	148.60.3.101	34.213.151.15	TCP	68	49130 → 443 [ACK] Seq=1 Ack=1 Win=309 Len=0 TSval=7183621 TSecr=885084795
27	1.376508373	93.184.220.29	148.60.3.101	TCP	68	[TCP ACKed unseen segment] 80 → 45768 [ACK] Seq=1 Ack=2 Win=290 Len=0 TSval=1363645172 TSecr=2655038225
29	1.540176464	34.213.151.15	148.60.3.101	TCP	68	[TCP ACKed unseen segment] 443 → 49130 [ACK] Seq=1 Ack=2 Win=124 Len=0 TSval=885087401 TSecr=7163192
31	1.653941630	127.0.0.1	127.0.0.1	TCP	474	49162 → 9000 [PSH, ACK] Seq=1 Ack=1 Win=359 Len=406 TSval=2698459485 TSecr=2698456486
32	1.654298320	127.0.0.1	127.0.0.1	TCP	108	9000 → 49162 [PSH, ACK] Seq=1 Ack=407 Win=3637 Len=40 TSval=2698459486 TSecr=2698459485
33	1.654319238	127.0.0.1	127.0.0.1	TCP	68	49162 → 9000 [ACK] Seq=407 Ack=41 Win=359 Len=0 TSval=2698459486 TSecr=2698459486
34	1.733410054	148.60.3.101	148.60.3.101	TCP	68	33244 → 8031 [PSH, ACK] Seq=198 Ack=44 Win=342 Len=0 TSval=3715091301 TSecr=3715090280

Question 2 :

Le contenu du champ type de la trame Ethernet II est **IPv4(0x0800)** dans le champs **Ethernet II**.

```
▼ Ethernet II, Src: IntelCor_54:0b:00 (e0:94:67:54:0b:00), Dst: Sagemcom_69:81:03 (7c:26:64:69:81:03)
  > Destination: Sagemcom_69:81:03 (7c:26:64:69:81:03)
  > Source: IntelCor_54:0b:00 (e0:94:67:54:0b:00)
  Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.1.10, Dst: 129.20.126.118
```

Question 3 :

Adresse Ethernet destination : **7c:26:64:69:81:03**

Adresse IP destination : **129.20.126.118**

```
Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 129.20.126.118
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
```

Question 4 :

L'identifiant O.U.I de ma carte réseaux serait **IntelCorporation_54:0b:00**.

L'identifiant O.U.I de destination serait **Sagemcom_69:81:03**.

```
> Destination: Sagemcom_69:81:03 (7c:26:64:69:81:03)
> Source: IntelCor_54:0b:00 (e0:94:67:54:0b:00)
```

Question 5 :

Dans l'onglet **Internet Protocol** nous trouvons l'information de l'en-tête du paquet IP comme étant de **20 bytes (header length)**. La longueur total de ce paquet IP est de **52 bytes (total length)**.

```
▼ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 129.20.126.118
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x5eae (24238)
```

COMPTE RENDU TP1 RSP

Question 6 :

Les données transportées par le paquet IP sont destinées au **port 443** qui correspond au service **https**. On trouve cette information dans l'onglet **Transmission Control Protocol** dans le champs **Destination Port**.

```
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 59886, Dst Port: 443, Seq: 1772, Ack: 33361, Len: 0
Source Port: 59886
Destination Port: 443
[Stream index: 13]
[TCP Segment Len: 0]
Sequence number: 1772 (relative sequence number)
Acknowledgment number: 33361 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
```

Question 7 :

On trouve le champ **Time-To-Live** dans l'onglet **Internet Protocol**. Celui-ci à pour valeur **128**.

```
> Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
```