Examen Administration des Systèmes et des Réseaux
Durée 2 heures
Documents autorisés
Portables, ordinateurs et téléphones, éteints

J-M Moreno

Mardi 24 mars 2015

Attention

Sauf indication contraire, les questions sont indépendantes. Vous devez expliciter et argumenter vos réponses. Par ailleurs il n'y a pas forcément de « bonne » réponse, ou même de réponse, l'argumentation que vous adosserez à vos commentaires n'en sera que plus importante.

1 Nous avons ici le résultat de deux commandes *ifconfig*. Pour rappel la commande *ifconfig* permet de configurer ou de visualiser des interfaces réseaux avec leurs paramètres. C'est cette dernière possibilité que nous utilisons ici. Et entre les deux un appel à *tcpdump* qui permet de tracer le trafic du réseau. Pour alléger la présentation quelques éléments d'affichage sans importance ici ont été supprimés.

```
# ifconfig hme0
hme0: flags=68863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,NOINET6,INET6_NOPRIVACY> mtu 1500
        lladdr 08:00:20:da:4f:ac
        media: Ethernet autoselect (100baseTX full-duplex)
        status: active
        inet 194.254.199.47 netmask 0xffffff00 broadcast 194.254.199.255
# tcpdump ether host 08:00:20:da:4f:ac or 78:19:f7:10:ea:81 and ip6
tcpdump: listening on hme0, link-type EN10MB
16:10:23.231559 :: > ff02::1:ffda:4fac: icmp6:neighbor sol:who has fe80::a00:20ff:feda:4fac
16:10:25.892248 fe80::a00:20ff:feda:4fac > ff02::2: icmp6:router solicitation
16:10:26.310351 fe80::7a19:f7ff:fe10:ea81 > ff02::1: xicmp6:router advertisement
16:10:26.316070 :: > ff02::1:ffda:4fac: icmp6:neighbor sol:who has 2001:660:3301:8070:a00:20ff:feda:4fac
^C
103 packets received by filter
0 packets dropped by kernel
# ifconfig hme0
hme0: flags=248863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,INET6_NOPRIVACY,AUTOCONF6> mtu 1500
        lladdr 08:00:20:da:4f:ac
        media: Ethernet autoselect (100baseTX full-duplex)
        status: active
        inet 194.254.199.47 netmask 0xffffff00 broadcast 194.254.199.255
        inet6 fe80::a00:20ff:feda:4fac%hme0 prefixlen 64 scopeid 0x1
        inet6 2001:660:3301:8070:a00:20ff:feda:4fac prefixlen 64 autoconf pltime 604792 vltime 2591992
#
```

La question porte ici sur la configuration *IPv6*. Entre ces deux invocations de *ifconfig* il s'est produit un évènement, tracé par l'invocation de *tcpdump*. Pourriez-vous expliquer ce qu'il s'est passé ? Par ailleurs, sachant que l'adresse *Ethernet 08 :00 :20 :da :4f :ac* est celle de l'interface de la machine, à qui doit appartenir l'adresse *78 :19 :f7 :10 :ea :81* selon vous ?

2 De façon identique à la question précédente, nous avons ici le résultat de deux commandes *ifconfig* avec, entre les deux invocations une écoute du réseau à l'aide de *tcpdump*.

```
# ifconfig le0
le0: flags=28863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,NOINET6> mtu 1500
        lladdr 08:00:20:83:60:b0
        media: Ethernet autoselect (10baseT)
        status: active
        inet 192.168.70.96 netmask 0xffffff00 broadcast 192.168.70.255
# tcpdump ether host 08:00:20:83:60:b0 or 78:19:f7:10:ea:81 and ip6
tcpdump: listening on le0, link-type EN10MB
15:25:57.966033 :: > ff02::1:ff83:60b0: icmp6: neighbor sol: who has fe80::a00:20ff:fe83:60b0
15:26:00.286558 fe80::a00:20ff:fe83:60b0 > ff02::2: icmp6: router solicitation
15:26:04.295711 fe80::a00:20ff:fe83:60b0 > ff02::2: icmp6: router solicitation
15:26:08.305311 fe80::a00:20ff:fe83:60b0 > ff02::2: icmp6: router solicitation
^C
44 packets received by filter
0 packets dropped by kernel
# ifconfig le0
le0: flags=208863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,AUTOCONF6> mtu 1500
        lladdr 08:00:20:83:60:b0
        media: Ethernet autoselect (10baseT)
        status: active
        inet 192.168.70.96 netmask 0xffffff00 broadcast 192.168.70.255
        inet6 fe80::a00:20ff:fe83:60b0%le0 prefixlen 64 scopeid 0x1
#
```

Attention l'interface qui est tracée ici est bien *le0*[1] a ne pas confondre avec l'interface de boucle locale *lo0*. Comme précédemment on ne s'intéresse ici qu'à la configuration *IPv6*. Expliquez ce qu'il s'est produit ici, et aussi surtout ce qu'il ne s'est pas produit.

3 Nous allons ici en terminer avec *IPv6*. Voici une autre configuration obtenue à l'aide de *ifconfig* :

```
# ifconfig hme0
hme0: flags=8863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        lladdr 08:00:20:da:4f:ac
        media: Ethernet autoselect (100baseTX full-duplex)
        status: active
        inet 194.254.199.47 netmask 0xffffff00 broadcast 194.254.199.255
        inet6 fe80::a00:20ff:feda:4fac%hme0 prefixlen 64 scopeid 0x1
        inet6 2001:660:3301:8070::47 prefixlen 64
#
```

Que remarquez vous de particulier dans l'adresse *IPv6* de cette machine ? Quelle peut-être la raison de cette particularité, à votre avis ?

4 Dans ce qui suit nous allons nous intéresser à la configuration *IPv4*. Ceci est encore le résultat d'une invocation à *ifconfig* :

```
# ifconfig vlan929
vlan929: flags=28843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,NOINET6> mtu 1500
        lladdr 08:00:20:da:4f:ac
        vlan: 929 parent interface: hme0
        groups: vlan
```

[1] L'interface **le0** est basée sur un chipset *AMD*, tandis que l'interface **hme0** de la question précédente était basée sur un chipset *Sun*. Tout cela n'a strictement aucune importance ici.

```
        status: active
        inet 192.168.70.97 netmask 0xffffff00 broadcast 192.168.70.255
#
```

Que pourriez-vous dire sur l'interface *vlan929* ? Donnez tous les éléments que vous pourrez tirer de cet affichage[2].

5 Le protocole *LLDP*, *Link Layer Discovery Protocol*, situé au niveau 2 permet d'obtenir des informations sur le dispositif auquel est connecté un appareil. La commande *ladvdc* en est l'expression sous forme de client. Nous avons ci-dessous une invocation de cette commande :

```
# ladvdc
Capability Codes:
        r - Repeater, B - Bridge, H - Host, R - Router, S - Switch,
        W - WLAN Access Point, C - DOCSIS Device, T - Telephone, O - Other
Device ID                       Local Intf    Proto   Hold-time    Capability    Port ID
switch-baie1                    hme0          LLDP    98           B             6
#
```

Cela indique que l'interface *hme0* de la machine est connectée sur le port 6 du switch *switch-baie1*, les autres informations n'ont pas d'importance ici. L'affichage qui suit contient la configuration de ce port sur ce switch. Commentez le.

```
switch-baie1# show vlans ports 6 detail
 Status and Counters - VLAN Information - for ports 6
  Port name: moumoune
  VLAN ID Name                 Status       Jumbo Mode
  ------- -------------------- ------------ ----- --------
  581     ufop7                Port-based   No    Untagged
  929     rc07                 Port-based   No    Tagged
switch-baie1#
```

Si l'on suppose que les interfaces *hme0*, de la première question, et *vlan929* sont connectées sur ce port, cela vous parait il cohérent ? Expliquez et commentez.

6 Ce qui suit est la description d'une machine, tout d'abord grâce à *sysctl* qui permet d'obtenir — et de modifier — des paramètres du noyau, et ensuite grâce à *dmesg* qui fournit les messages du noyau. En particulier ceux du *boot* qui nous intéressent ici.

```
pois-chiche# sysctl hw.model hw.machine hw.ncpu hw.physmem
hw.model=Intel(R) Xeon(R) CPU E5-2420 v2 @ 2.20GHz
hw.machine=amd64
hw.ncpu=24
hw.physmem=51475578880
pois-chiche# dmesg | head -3
OpenBSD 5.6 (GENERIC.MP) #333: Fri Aug  8 00:20:21 MDT 2014
    deraadt@amd64.openbsd.org:/usr/src/sys/arch/amd64/compile/GENERIC.MP
real mem = 51475578880 (49090MB)
pois-chiche#
```

Les différentes informations parlent d'elles-mêmes, précisons néanmoins que *hw.ncpu* donne le nombre de *CPU* et *hw.physmem* la taille mémoire. Pour vous éviter de faire le calcul : $51\,475\,578\,880$ **octets correspondent à 48 Go de mémoire. Enfin le fait que le système soit déclaré *MP*, veut dire qu'on utilise la version multi-processeur. Dites ce que vous pensez de cette configuration et à quoi elle pourrait servir. Justifiez vos réponses. Si vous pensez qu'il manque des éléments pour affiner votre réponse dites lesquels.**

[2] Il serait judicieux que vous remarquiez que l'adresse **Ethernet** *08 :00 :20 :da :4f :ac* apparaît dans la première question.

7 **Voici dans ce qui suit une liste restreinte de processus s'exécutant sur une machine. L'option *-U* de *ps* permet de restreindre l'affichage à un utilisateur particulier. Le *pipe* avec la commande *grep -v grep*, ne sert qu'à nettoyer l'affichage. Ainsi que les informations sur un logiciel.**

```
root     18001  0.0  0.0  1616   440 p0  R      3:00PM    0:00.00 grep httpd (tcsh)
# ps -U_mysql ; ps -auxw | grep httpd | grep -v grep
  PID TT  STAT       TIME COMMAND
20321 p1  I      34:13.40 /usr/local/libexec/mysqld --basedir=/usr/local --datadir=/var/mysql
root      3642  0.0  0.0  6140 17280 ??  Ss    Thu01PM    0:06.68 /usr/local/apache2/bin/httpd
www      29406  0.0  0.0 23548 13140 ??  I     Mon03PM    0:17.32 /usr/local/apache2/bin/httpd
www      15727  0.0  0.1 36784 26176 ??  I     Mon03PM    0:14.37 /usr/local/apache2/bin/httpd
www       9062  0.0  0.1 44740 32612 ??  I     Mon03PM    0:16.51 /usr/local/apache2/bin/httpd
```

À cela nous rajouterons cette information :

```
# php --version
PHP 5.6.6 (cli) (built: Mar  2 2015 16:46:45)
Copyright (c) 1997-2015 The PHP Group
Zend Engine v2.6.0, Copyright (c) 1998-2015 Zend Technologies
    with Suhosin v0.9.37.1, Copyright (c) 2007-2014, by SektionEins GmbH
#
```

Pourriez-vous dire quel type d'applications semble exécuter cette machine ? Justifiez votre réponse. Quelle devrait être selon vous la configuration de cette machine ? Par le plus grand des hasards, et la plus heureuse des coïncidences, pensez qu'il y ait dans une des questions de ce sujet une description de machine correspondante ? Si oui dites pourquoi ? Si non dites pourquoi ?

8 **On affiche ici un échantillon des journaux de consignation — les *logs* — d'un routeur, plus précisément ceux du filtrage d'accès. Les invocations de *sed*, *egrep*, *egrep*, *head* et *tail* permettent de réaliser l'échantillonnage. L'affichage a été un peu élagué pour plus de clarté.**

```
% cat juniper.log | sed -f sed.txt | egrep 'destination-p.+ 80' | grep 128.61.240.66 | head -5
Mar 16 09:09:52 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.73 source-port 60000 destination-port 80 (count 1 packet)
Mar 16 09:10:28 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.51 source-port 60000 destination-port 80 (count 1 packet)
Mar 16 09:10:43 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.102 source-port 60000 destination-port 80 (count 1 packet)
Mar 16 09:10:56 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.36 source-port 60000 destination-port 80 (count 1 packet)
Mar 16 09:11:11 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.23 source-port 60000 destination-port 80 (count 1 packet)
% cat juniper.log | sed -f sed.txt | egrep 'destination-p.+ 80' | grep 128.61.240.66 | tail -5
Mar 19 13:57:56 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.116 source-port 60000 destination-port 80 (count 1 packet)
Mar 19 13:58:35 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.83 source-port 60000 destination-port 80 (count 1 packet)
Mar 19 15:25:34 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.8 source-port 60000 destination-port 80 (count 1 packet)
Mar 19 15:26:49 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 194.254.199.23 source-port 60000 destination-port 80 (count 1 packet)
Mar 19 15:35:43 : interface-name ge-0/0/2.0 action D protocol-name tcp source-address 128.61.240.66
destination-address 195.254.199.21 source-port 60000 destination-port 80 (count 1 packet)
%
```

L'affichage est simple : l'action *D* provient de *Denied*, l'adresse source (c'est-à-dire celle qui veut se connecter), l'adresse de destination et enfin les ports source et de destination. Ce dernier nous intéresse, pourriez-vous dire à quel protocole est alloué le port 80 ? Selon vous qu'est-il en train de se passer ? Justifiez votre réponse.