M1 RES - Travaux sur machine encadrés 6/10

Couche réseau : IP, ICMP...

Nous nous intéressons à la couche réseau dans l'environnement TCP/IP. Lors des scéances précédente, nous avons déjà observé de nombreux de paquets IP dans les traces analysées. Nous nous attacherons donc à observer du trafic spécifique à la couche 3 à travers deux outils fondamentaux pour la supervision des réseaux TCP/IP : `ping` et `traceroute`.

1 Etude de l'outil `ping`

Voici le début de la description du `man` UNIX sur la commande `ping` :

> `Ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (``pings'') have an IP and ICMP header, followed by a ``struct timeval'' and then an arbitrary number of ``pad'' bytes used to fill out the packet.`

1.1 Test d'une machine distante

La commande `ping` permet de tester la connectivité vers une machine distante, et — en envoyant plusieurs paquets à la suite — d'effectuer des statistiques sur les caractéristiques du chemin suivi (RTT, taux de perte, variabilité des résultats en fonction de la taille des datagrammes émis...). Voici un exemple d'utilisation :

```
pirogue:~# ping sphinx.lip6.fr
PING sphinx.lip6.fr (132.227.74.253): 56 data bytes
64 bytes from 132.227.74.253: icmp_seq=0 ttl=247 time=5.5 ms
64 bytes from 132.227.74.253: icmp_seq=1 ttl=247 time=9.3 ms
64 bytes from 132.227.74.253: icmp_seq=2 ttl=247 time=8.0 ms
64 bytes from 132.227.74.253: icmp_seq=3 ttl=247 time=6.3 ms
64 bytes from 132.227.74.253: icmp_seq=4 ttl=247 time=4.8 ms
64 bytes from 132.227.74.253: icmp_seq=5 ttl=247 time=7.6 ms
64 bytes from 132.227.74.253: icmp_seq=6 ttl=247 time=5.8 ms

--- sphinx.lip6.fr ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 4.8/6.7/9.3 ms
pirogue:~#
```

1. Pour vous échauffer, analysez **manuellement** (sans `ethereal`) la première trame correspondant à cet échange :

```
0000  00 08 21 59 66 42 00 04  76 21 1b 95 08 00 45 00   ..!YfB.. v!....E.
0010  00 54 64 db 00 00 40 01  df 38 c2 fe a3 b6 84 e3   .TdÛ..@. ß8Âþ£¶.ã
0020  4a fd 08 00 d8 2d 6e 5b  00 00 3f 9f 10 01 00 0d   Jý..Ø-n[ ..?.....
0030  76 c6 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   vÆ...... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

2. A votre avis, a quoi correspondent les données transportées par le messages ICMP analysé précédement ? Utilisez le `man` UNIX pour avoir des informations complémentaires sur `ping`.
3. Utilisez à présent le logiciel `ethereal` pour la suite.
   Chargez le fichier suivant : `/Infos/lmd/2004/master/ue/res-2004oct/tme6-pin.dmp.gz`.
   Quel échange observez vous dans cette trace ?
4. Quelle réponse est retournée à la requête analysée précédement ?
5. Analysez les champs ICMP de plusieurs paquets échangées. Développez leur signification et inférez leur utilité pour la commande `ping`.

1.2 Test d'une machine proche avec enregistrement du chemin

La commande `ping -R` est une variante de l'exécution illustrée précédement où des option de l'entête IP sont introduites. A vous de les découvrir dans l'exemple suivant :

```
pirogue:~# ping -R rap-jussieu.cssi.renater.fr
PING rap-jussieu.cssi.renater.fr (193.51.182.201): 56 data bytes
64 bytes from 193.51.182.201: icmp_seq=0 ttl=252 time=11.2 ms
RR:     pirogue.l2ti.univ-paris13.fr (194.254.163.182)
        192.168.208.252
        paris13-jussieu.cssi.renater.fr (193.51.182.205)
        jussieu-a1-0-65.cssi.renater.fr (193.51.182.202)
        rap-jussieu.cssi.renater.fr (193.51.182.201)
        jussieu-f3-3.cssi.renater.fr (193.51.182.206)
        192.168.208.254
        gw163.univ-paris13.fr (194.254.163.254)
        pirogue.l2ti.univ-paris13.fr (194.254.163.182)

--- rap-jussieu.cssi.renater.fr ping statistics ---
5 packets transmitted, 1 packets received, 80% packet loss
round-trip min/avg/max = 11.2/11.2/11.2 ms
pirogue:~#
```

1. Chargez le fichier suivant : `/Infos/lmd/2004/master/ue/res-2004oct/tme6-pRp.dmp.gz`.
   Quel informations nouvelles découvrez vous dans ces trames ?
2. Analysez les champs ICMP. Développez leur signification et inférez, avec le contenu de l'option IP, leur utilité pour la commande `ping -R`.
3. Pouvez-vous réaliser un schéma des réseaux traversés ?

1.3 Test d'une machine éloignée avec enregistrement du chemin

La commande `ping -R` utilise le champ d'option limité de l'entête IP. Que se passe-t'il dans l'exemple suivant ?

```
pirogue:~# ping -R sphinx.lip6.fr
PING sphinx.lip6.fr (132.227.74.253): 56 data bytes
64 bytes from 132.227.74.253: icmp_seq=0 ttl=247 time=8.8 ms
RR:     pirogue.l2ti.univ-paris13.fr (194.254.163.182)
        192.168.208.252
        paris13-jussieu.cssi.renater.fr (193.51.182.205)
        jussieu-a1-0-65.cssi.renater.fr (193.51.182.202)
        gw-rap.rap.prd.fr (195.221.126.78)
        rap-jussieu.rap.prd.fr (195.221.127.181)
        r-jusren.reseau.jussieu.fr (134.157.254.126)
        r-olympe.lip6.fr (132.227.109.254)
        132.227.74.254
64 bytes from 132.227.74.253: icmp_seq=1 ttl=247 time=3099.5 ms (same route)
64 bytes from 132.227.74.253: icmp_seq=2 ttl=247 time=2099.7 ms (same route)
64 bytes from 132.227.74.253: icmp_seq=3 ttl=247 time=1099.9 ms (same route)
```

```
64 bytes from 132.227.74.253: icmp_seq=4 ttl=247 time=100.1 ms  (same route)
64 bytes from 132.227.74.253: icmp_seq=5 ttl=247 time=8.6 ms    (same route)
64 bytes from 132.227.74.253: icmp_seq=6 ttl=247 time=14.0 ms   (same route)

--- sphinx.lip6.fr ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 8.6/918.6/3099.5 ms
pirogue:~#
```

1. Chargez le fichier suivant : `/Infos/lmd/2004/master/ue/res-2004oct/tme6-pRl.dmp.gz`.
   Quel informations nouvelles découvrez vous dans ces trames ?
2. Analysez la route enregistrée dans les paquets IP de retour. Quelles différences observez vous ?
3. Quelle limitations constatez vous pour l'approche `ping -R` pour déduire la route suivie par les paquets vers un destinataire donné ?

2 Etude de l'outil `traceroute`

Voici le début de la description du `man` UNIX sur la commande `traceroute` :

> `The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one's packets follow (or finding the miscreant gateway that's discarding your packets) can be difficult. Traceroute utilizes the IP protocol 'time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host.`

La commande `traceroute` permet de récupérer les adresses des interfaces des machines intermédaires vers une machine distante. Voici un exemple d'utilisation :

```
pirogue:~# traceroute sphinx.lip6.fr
traceroute to sphinx.lip6.fr (132.227.74.253), 30 hops max, 38 byte packets
 1  gw163.univ-paris13.fr (194.254.163.254)  2.579 ms  0.496 ms  0.415 ms
 2  192.168.208.254 (192.168.208.254)  0.640 ms  0.602 ms  0.216 ms
 3  jussieu-f3-3.cssi.renater.fr (193.51.182.206)  1.813 ms  2.100 ms  1.778 ms
 4  rap-jussieu.cssi.renater.fr (193.51.182.201)  1.986 ms  2.167 ms  2.216 ms
 5  cr-jussieu.rap.prd.fr (195.221.126.77)  2.867 ms  2.799 ms  2.642 ms
 6  jussieu-rap.rap.prd.fr (195.221.127.182)  3.021 ms  3.797 ms  2.315 ms
 7  r-scott.reseau.jussieu.fr (134.157.254.10)  3.692 ms  4.402 ms  5.438 ms
 8  olympe-gw.lip6.fr (132.227.109.1)  4.881 ms !N  3.932 ms !N  3.917 ms !N
pirogue:~#
```

1. Chargez le fichier suivant : `/Infos/lmd/2004/master/ue/res-2004oct/tme6-tcr.dmp.gz`.
   Analysez la première trame `traceroute` envoyée. Quel est son but ?
2. Quel evenement génère la trame suivante ? Quel intéret peut on retirer de ce phénomène ?
3. A votre avis, de quelle manière la commande `traceroute` génère-t-elle ses réponses ?
4. Pourquoi les numéros de port UDP destination évoluent'ils ?
5. Finalement, de quelle manière la commande `traceroute` termine-t-elle ?