M1 RES - Travaux sur machine encadrés 7/10

Routage + VLAN

Nous nous intéressons toujours à la couche réseau et, en particulier, aux protocoles de **routage** dans l'environnement TCP/IP. Lors des séances précédentes, nous avons observé de nombreux paquets IP dans les traces analysées. Ici, nous nous attacherons à étudier du trafic généralement échangé entre routeurs pour deux protocoles : RIP et BGP.

1 Protocole de routage interne : RIP

1. Pour vous échauffer, analysez **manuellement** (sans `ethereal`) cette première trame. Détaillez les différentes encapsulations présentes :

```
0000  01 00 5e 00 00 09 00 08  c7 a4 d4 be 08 00 45 00   ..^..... ......E.
0010  00 98 73 2f 00 00 01 11  74 38 84 e3 6d 01 e0 00   ..s/.... t8..m...
0020  00 09 02 08 02 08 00 84  29 77 02 02 00 00 00 02   ........ )w......
0030  00 00 84 e3 3d 00 ff ff  ff 00 00 00 00 00 00 00   ....=... ........
0040  00 01 00 02 00 00 84 e3  3e 00 ff ff ff 00 00 00   ........ >.......
0050  00 00 00 00 00 01 00 02  00 00 84 e3 48 00 ff ff   ........ ....H...
0060  ff 00 00 00 00 00 00 00  00 01 00 02 00 00 84 e3   ........ ........
0070  4a 00 ff ff ff 00 00 00  00 00 00 00 00 01 00 02   J....... ........
0080  00 00 84 e3 6b 00 ff ff  ff 00 00 00 00 00 00 00   ....k... ........
0090  00 01 00 02 00 00 84 e3  6e 00 ff ff ff 00 00 00   ........ n.......
00a0  00 00 00 00 00 01                                  ......
```

2. Généralement, les protocoles de routage diffusent leurs informations. Pour cela des adresses de diffusion *(broadcast)* sont utilisées. Ici RIPv2 est utilisé. Ce dernier favorise la diffusion limitée *(multicast)*. Typiquement, ce type d'adresse se reconnaît au niveau de la couche MAC par le premier bit d'adresse transmit à `1` et au niveau de la couche IP par les 4 bits de poids fort du premier octet de l'adresse positionné à `0xE` (ex-classe D). Que pouvez vous dire à propos des adresses présentes dans la trame ci-dessus ?
3. Justifiez la valeur du TTL ?
4. A votre avis, quel est le mécanisme de fiabilité mis en œuvre ?
5. Vous n'avez pas d'information sur la structure de la couche applicative transportée. Sachant ce que doit transporter un protocole de routage basé sur les vecteurs de distances pour IP avec un adressage CIDR, faites donc un peu de *reverse engineering* – tant que cela est autorisé en Europe – pour déduire les champs transportés.
6. Utilisez à présent le logiciel `ethereal` pour le fichier `/Infos/lmd/2004/master/ue/res-2004oct/tme-rip.dmp.gz`. Qu'observez vous dans cette trace ?
7. Confirmez les hypothèses d'analyse des divers champs des messages du protocole RIP.
8. A votre avis, quel serait le vecteur construit à son tour par le routeur suivant après avoir reçut les messages observés ?

2 Protocole de routage externe : BGP

1. Pour ne pas vous refroidir, analysez encore **manuellement** la trame suivante :

```
0000  00 00 0c 35 0e 1c 00 c0  4f 23 c5 95 08 00 45 00   ...5.... O#....E.
0010  00 45 48 e9 40 00 40 06  70 49 c0 a8 00 0f c0 a8   .EH.@.@. pI......
0020  00 21 08 4c 00 b3 d6 33  9d 62 7a 40 e0 46 50 18   .!.L...3 .bz@.FP.
0030  7d 78 19 03 00 00 ff ff  ff ff ff ff ff ff ff ff   }x...... ........
0040  ff ff ff ff ff ff 00 1d  01 04 fe 09 00 b4 c0 a8   ........ ........
0050  00 0f 00                                          ...
```

2. Quelles différences observez vous par rapport à l'échange d'information RIP ? Justifier.
3. Utilisez à nouveau `ethereal` pour le fichier suivant : `/Infos/lmd/2004/master/ue/res-2004oct/tme7-bgp.dmp.gz`. Quel échange observez vous dans cette trace ?
4. Quelle est la signification des messages successivement échangés ?
5. Si le trafic RIP observé précédement atteignait le routeur BGP de bordure de son AS, quel type d'information pourrait être alors observée dans la connexion BGP ?

3 Etude de trafic de VLAN *(facultatif)*

1. Utilisez le logiciel `ethereal` pour le fichier : `/Infos/lmd/2004/master/ue/res-2004oct/tme7-vlan.dmp.gz`. Qu'observez vous dans cette trace ?
2. Définissez les grandes catégories de trafic observés.
3. Pouvez vous les regrouper grâce à un découpage logique du réseau ?
4. Ces trafics peuvent-ils communiquer entre eux ?