



Réseaux IP

Bridging & Spanning-Tree

Auteurs :

M. Samuel RIEDO
M. Maic QUEIROZ

Encadrant :

M. François BUNTSCHU

Introduction

Problème 1

Quelles sont les adresses contenues dans les tables d'acheminement ?

- e840.f2ac.c6c0 (PC)
- 0015.f9f6.e7e8
- e840.f2ac.c75a (PC)
- e840.f2ac.c20c (PC)

Les trois PCs sont présents dans la table (aucun portable n'est connecté au réseau). L'OUI e8 :40 :f2 correspond au fabricant PEGATRON CORPORATION. La dernière adresse correspond à un "bruit de fond", son OUI étant celui de Cisco. Tous les appareils ayant communiqué récemment sont présent dans la table.

```
bridge_y#sh bridge
Total of 300 station blocks, 295 free
Codes: P - permanent, S - self
Bridge Group 1:

```

Address	Action	Interface	Age	RX count	TX count
e840.f2ac.c6c0	forward	Gi0/1	0	327	0
0015.f9f6.e7e8	forward	Gi0/1	3	1	0
4c00.827e.dfe0	forward	Gi0/1	0	1	0
e840.f2ac.c75a	forward	Gi0/1	0	208	0
e840.f2ac.c20c	forward	Gi0/1	3	2	0

```
bridge_y#sh bridge
```

FIGURE 1 – Table d'acheminement

Problème 2

Analyser (capturer) et commenter/décrire le trafic (trames) Spanning Tree.

Une trame STP (Spanning-Tree Protocol) est émise à intervalle de deux secondes par le routeur root. Chaque routeur recevant la trame STP la renvoie sur ses autres interfaces. Ainsi, sur chaque analyseur Wireshark, la source des trames STP est différente.

Dans notre cas, notre routeur est en bout de ligne, il reçoit donc sur son interface 0/1 les trames STP du routeur root, et sur son interface 0/1 les trames ré-émises du root par le routeur de la table x. De ce fait, il n'a pas à émettre de trame STP.

```

Spanning Tree Protocol
  Protocol Identifier: Spanning Tree Protocol (0x0000)
  Protocol Version Identifier: Spanning Tree (0)
  BPDU Type: Configuration (0x00)
  > BPDU flags: 0x00
  ✓ Root Identifier: 32768 / 0 / 00:15:f9:f6:e7:e8
    Root Bridge Priority: 32768
    Root Bridge System ID Extension: 0
    Root Bridge System ID: CiscoInc_f6:e7:e8 (00:15:f9:f6:e7:e8)
    Root Path Cost: 100
  ✓ Bridge Identifier: 32768 / 0 / 4c:00:82:7e:df:e0
    Bridge Priority: 32768
    Bridge System ID Extension: 0
    Bridge System ID: CiscoInc_7e:df:e0 (4c:00:82:7e:df:e0)
  Port identifier: 0x8004
  Message Age: 1
  Max Age: 20
  Hello Time: 2
  Forward Delay: 15

```

FIGURE 2 – Spanning Tree

Problème 3

Un tel réseau peut-il fonctionner sans le protocole de gestion des bridges (STP) ? Pourquoi ?

Non, car la présence de boucle, dans ce cas, va régénérer infiniment chaque trame émise par les PCs. Le protocole TTL (Time-To-Live) ne supprimera pas les trames après un certain nombre de bonds, car tous les équipement présents sont en couche 2 et seule ceux en couche 3 décrémentent le compteur.

Le medium sera donc occupé en permanence avec un nombre de collisions très élevé, empêchant les données d'être correctement transmises.

Problème 4

Quel est le root bridge ? Pourquoi ?

Le root est le routeur de la table z (adresse 00:15:f9:f6:e7:e8). Comme les trois routeurs ont été initialisés avec les valeurs Priority par défaut (32768), le routeur avec la plus petite adresse Mac est désigné comme root.

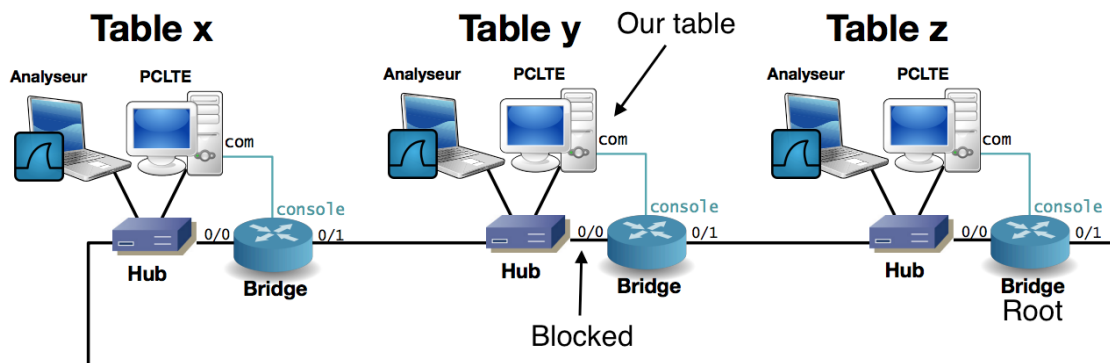


FIGURE 3 – Infrastructure du réseau

Problème 5

Quel port de quel bridge est bloqué par le Spanning Tree ? Pourquoi ?

Le routeur bridge_z est le root. Les interfaces 0/0 de bridge_x et 0/1 de bridge_y sont directement connectés dessus, elles sont donc des Root Port (RP).

Le choix de la ligne pour le sous réseau comportant le hub_y et le PC_y se fait donc entre l'interface 0/1 du bridge_x et l'interface 0/0 du bridge_y. Les deux bridges ayant la même valeur Priority, c'est celui avec le plus petit ID, donc la plus petite adresse Mac qui est choisit comme DB (Designed Bridge). Dans notre cas, c'est le bridge de la table x.

L'interface 0/0 de notre routeur (table y) est donc bloquée.

```
Port 3 <GigabitEthernet0/0> of Bridge group 1 is blocking
Port path cost 100, Port priority 128, Port Identifier 128.3.
Designated root has priority 32768, address 0015.f9f6.e7e8
Designated bridge has priority 32768, address 4c00.827e.dfe0
Designated port id is 128.4, designated path cost 100
Timers: message age 2, forward delay 0, hold 0
Number of transitions to forwarding state: 0
BPDU: sent 1, received 2241
```

FIGURE 4 – Interface bloquée

Problème 6

Les adresses IP sont-elles modifiées par le bridge ? Et les adresses MAC ? Coordonner une mesure avec la table voisine pour déterminer ces correspondances. Les adresses IP ne sont pas modifiées, et ne le sont jamais. Dans le cas contraire, les équipements ne seraient plus en mesure de savoir quel est la source ou le destinataire.

Pour ce qui est des adresses Mac, elles restent également identiques. Tous les équipements utilisés dans le TP sont en couche 2, ils ne les utilisent et modifient donc pas (notre routeur étant configuré en bridge).

icmp									
No.	Time	Source	Destination	Proto	Length	Info			
→ ...	10.494585	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2408/26633, ttl=128 (reply in 12)		
← ...	10.496455	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2408/26633, ttl=128 (request in 11)		
...	11.505553	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2409/26889, ttl=128 (reply in 14)		
...	11.507410	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2409/26889, ttl=128 (request in 13)		
...	12.515798	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2410/27145, ttl=128 (reply in 17)		
...	12.517683	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2410/27145, ttl=128 (request in 16)		
...	13.525895	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2411/27401, ttl=128 (reply in 19)		
...	13.527768	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2411/27401, ttl=128 (request in 18)		
...	14.536117	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2412/27657, ttl=128 (reply in 22)		
...	14.537966	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2412/27657, ttl=128 (request in 21)		
...	15.546346	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2413/27913, ttl=128 (reply in 24)		
...	15.548228	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2413/27913, ttl=128 (request in 23)		
...	16.556554	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2414/28169, ttl=128 (reply in 29)		
...	16.558466	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2414/28169, ttl=128 (request in 28)		
...	17.566657	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2415/28425, ttl=128 (reply in 31)		
...	17.568484	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2415/28425, ttl=128 (request in 30)		
...	18.576837	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2416/28681, ttl=128 (reply in 35)		
...	18.578702	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2416/28681, ttl=128 (request in 34)		
...	19.587011	192.168.0.60	192.168.0.70	ICMP	74	Echo (ping) request	id=0x0001, seq=2417/28937, ttl=128 (reply in 39)		
...	19.588878	192.168.0.70	192.168.0.60	ICMP	74	Echo (ping) reply	id=0x0001, seq=2417/28937, ttl=128 (request in 38)		

>	Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▼	Ethernet II, Src: Pegatron_ac:c2:0c (e8:40:f2:ac:c2:0c), Dst: Pegatron_ac:c6:c0 (e8:40:f2:ac:c6:c0)
>	Destination: Pegatron_ac:c6:c0 (e8:40:f2:ac:c6:c0)
>	Source: Pegatron_ac:c2:0c (e8:40:f2:ac:c2:0c)
>	Type: IPv4 (0x0800)

FIGURE 5 – Adresses des pings sur le PC A

FIGURE 6 – Adresses des pings sur le PC B

Problème 7

Que se passe-t-il ?

Sans le protocole STP, les bridges ne communiquent pas entre eux et ne sont pas en mesure de détecter la présence d'une boucle. De ce fait, aucune de leurs interfaces n'est bloquée.

Lorsque le premier ping est émis depuis la station x à destination de la station z, le bridge_x transfère les données sur ses deux interfaces, du fait qu'il ne sait pas où la station z se trouve. Ce paquet va ensuite arriver sur les bridges y et z. Ces derniers enregistrent dans leur table où se trouve la station x selon la provenance du paquet, et le transfèrent sur l'interface opposée.

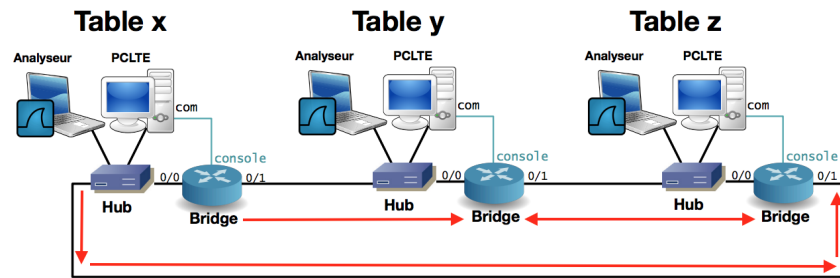


FIGURE 7 – Premières étapes de la transmission du paquet

A ce moment là, les bridges y et z vont recevoir la même trame qu'ils viennent d'envoyer, mais sur l'interface opposée à celle où ils l'ont reçue la première fois. L'adresse de la station x dans leur table de routage va donc changer, et ils vont retransmettre le paquet sur la même interface que la où il est arrivé (voir figure 7).

Le paquet va donc arriver sur les deux interfaces du bridge x (figure 8), ce dernier va donc le faire à nouveau transiter, revenant dans le même état que sur la figure 7.

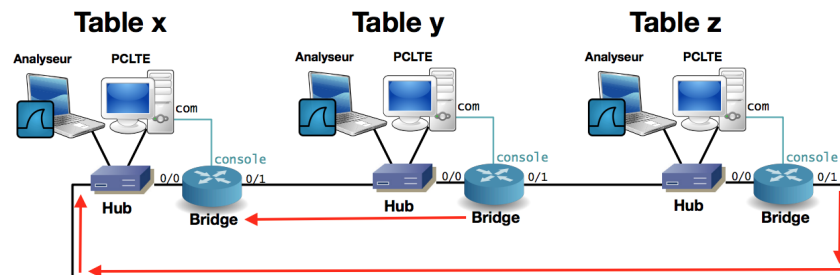


FIGURE 8 – Premières étapes de la transmission du paquet

Les paquets émis transistent donc sur le réseau de manière infinie.

Problème 8

Quel est le problème d'une boucle en couche 2 du modèle OSI par rapport à une boucle en couche 3 (IP) ?

Le protocole Time-To-Live n'est pas implémenté en couche 2, les paquets peuvent donc transiter à l'infini au travers du réseau. Si le même scénario était effectué avec des routeurs dans le circuit, à chaque fois qu'un paquet transiterait au travers de l'un d'eux, son compteur TTL serait décrementé. Dès qu'il atteindrait la valeur 0, le paquet ne serait plus transféré par les routeurs.

Conclusion

Table des figures

1	Table d'acheminement	1
2	Spanning Tree	1
3	Infrastructure du réseau	2
4	Interface bloquée	2
5	Adresses des pings sur le PC A	3
6	Adresses des pings sur le PC B	3
7	Premières étapes de la transmission du paquet	4
8	Premières étapes de la transmission du paquet	4

Fribourg, le 20 octobre 2016

Samuel Riedo

Maic Queiroz