S7

Réseaux IP

Réseaux Privés Virtuels (VPN)

Auteurs :
M. Samuel Riedo
M. Maic Queiroz

Encadrant :
M. François Buntschu

10 janvier 2017

Introduction

Lors de ce TP nous nous sommes intéressés au VPN (Virtual Private Network). Le VPN est un système permettant de créer un lien direct virtuel entre des ordinateurs ou des routeurs. De ce fait il permet d'étendre un réseau privé au travers d'un réseau public. Le VPN est de plus en plus utilisé notamment pour permettre le travail à distance.

Problème 1

Préparez un schéma de câblage et d'adressage de votre infrastructure.
Le matériel a été adressé et branché comme suit :

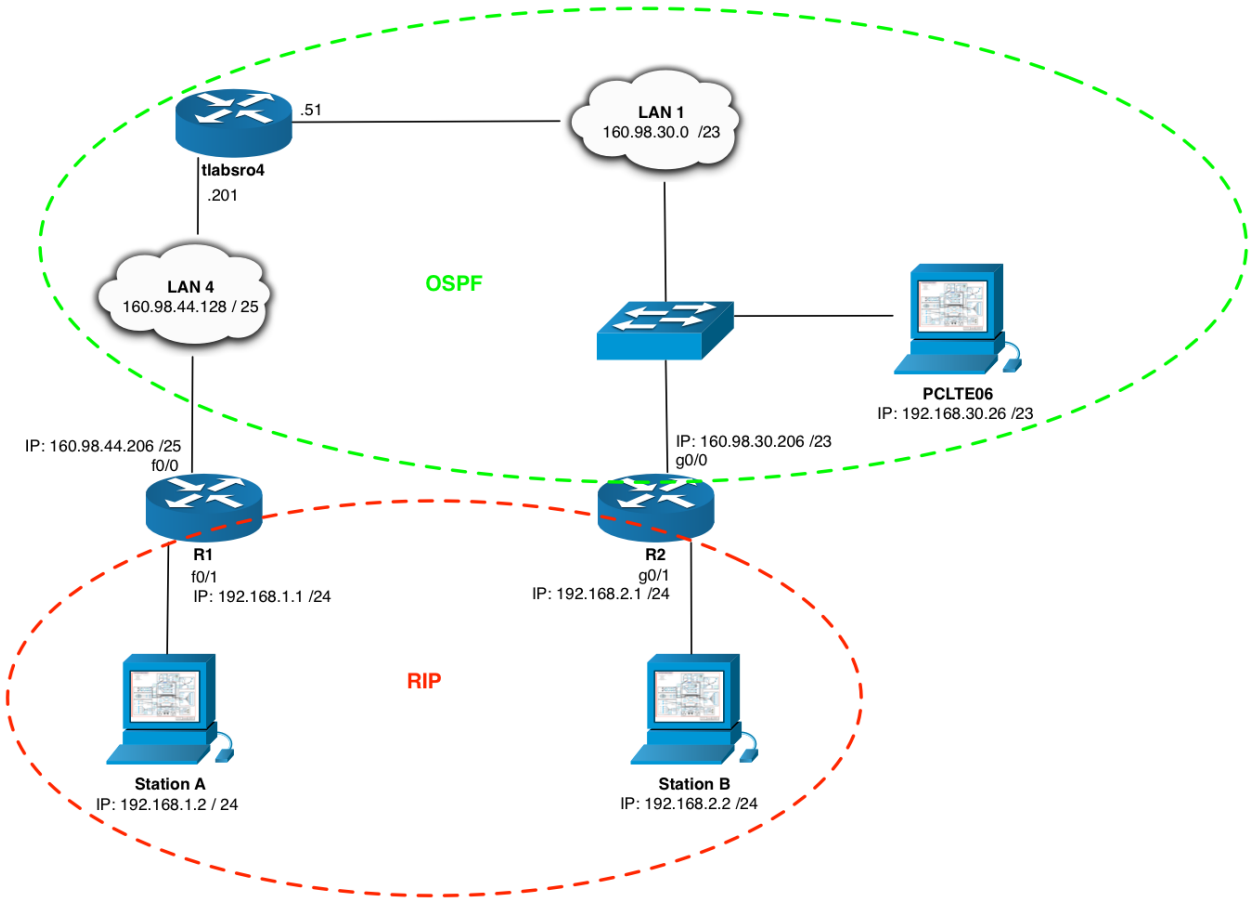

FIGURE 1 – Schéma d'adressage et de câblage

Problème 2

Pourquoi les stations A et B ne peuvent pas communiquer entre elles ? Quel type de message reçoit la station A ? Que faudrait-il mettre en place pour que cette communication soit possible ?

Les deux stations ne peuvent pas communiquer entre elles, car aucune route n'est connue entre les routeurs R1, R2 et tlabsro04. Les deux réseaux A et B ne peuvent donc pas être connecté entre eux. Afin de corriger ce problème, il faudrait par exemple configurer du NAT.

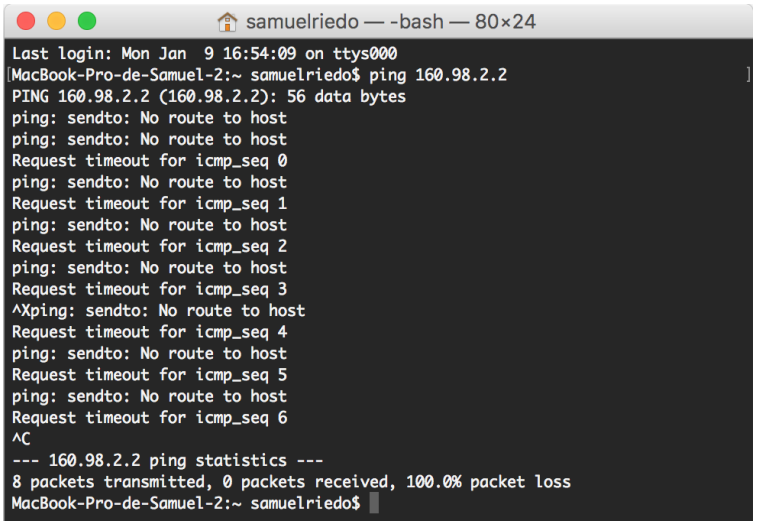

FIGURE 2 – Ping depuis A vers B

Problème 3

Quelles sont les tables de routage des routeurs R1 et R2 après avoir activé l'OSPF (show ip route) ? Décrivez les différentes entrées.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     160.98.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       160.98.44.128/25 is directly connected, FastEthernet0/0
O       160.98.30.0/23 [110/2] via 160.98.44.201, 00:01:26, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
R1#
```

FIGURE 3 – R1

```
r2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      160.98.0.0/16 is variably subnetted, 3 subnets, 3 masks
C        160.98.30.0/23 is directly connected, GigabitEthernet0/0
L        160.98.30.206/32 is directly connected, GigabitEthernet0/0
O        160.98.44.128/25
           [110/11] via 160.98.30.51, 00:01:54, GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/1
L        192.168.2.1/32 is directly connected, GigabitEthernet0/1
r2#
```

FIGURE 4 – R2

Comme nous pouvons le constater, nous avons 3 types de routes dans nos tables de routage :

- **C** : Il s'agit des subnets directement connectés à notre routeur.
- **O** : Il s'agit des routes échangées entre les différents routeurs à l'aide du protocole OSPF.
- **L** : Il s'agit des routes locales.

Problème 4

Validez que le routeur R1 puisse communiquer avec le routeur R2. Quelles adresses utilisez-vous pour ce test ? Justifiez.
L'adresse utilisée est celle de l'interface 0/0 du routeur, soit l'interface du côté OSPF ayant l'adresse *160.98.44.201*. Nous avons choisi d'émettre un ping sur cette interface du routeur, car l'autre n'était pas accessible à l'extérieur à ce moment là du TP.

```
R1#ping 160.98.44.201

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 160.98.44.201, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1#
```

FIGURE 5 – Ping entre R1 et R2

Problème 5

Pourquoi la station A ne peut pas communiquer avec la station B ? Que devez-vous mettre place pour que cela soit possible ?
Le routeur R1 ne connaît pas le subnet *192.168.2.0* et le routeur R2 ne connaît pas le subnet *192.168.1.0*. Il est donc nécessaire de rajouter les routes requises sur chacun de nos routeurs afin de leur permettre d'atteindre les subnets susmentionnés. Ces routes peuvent être statiques ou dynamiques (RIP, OSPF, ...).

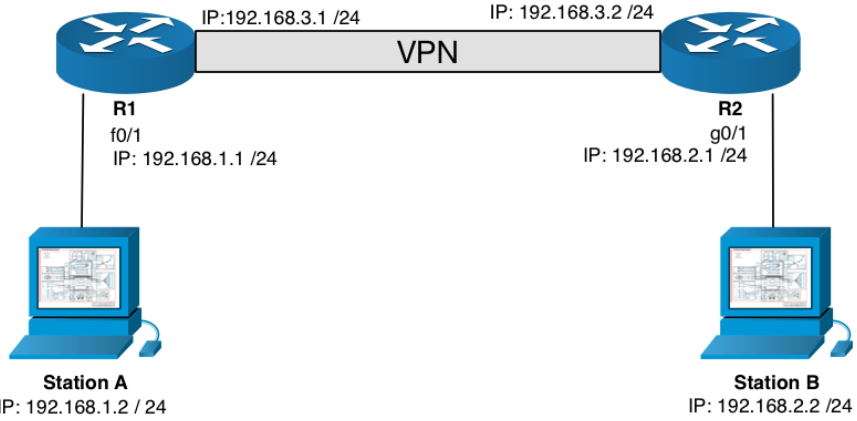

FIGURE 6 – Schéma VPN

Le VPN crée, d'un point de vue logique, une connexion directe entre les routeurs R1 et R2 comme si ces derniers étaient directement connectés entre eux avec un câble.

Problème 6

Quelles sont les tables de routage des routeurs R1 et R2 après avoir activé le RIP (show ip route) ? Décrivez les différentes entrées.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     160.98.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       160.98.44.128/25 is directly connected, FastEthernet0/0
O       160.98.30.0/23 [110/2] via 160.98.44.201, 00:51:40, FastEthernet0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/1
R    192.168.2.0/24 [120/1] via 192.168.3.2, 00:00:05, Tunnel0
C    192.168.3.0/24 is directly connected, Tunnel0
R1#
```

FIGURE 7 – R1

```
r2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      160.98.0.0/16 is variably subnetted, 3 subnets, 3 masks
C        160.98.30.0/23 is directly connected, GigabitEthernet0/0
L        160.98.30.206/32 is directly connected, GigabitEthernet0/0
O        160.98.44.128/25
           [110/11] via 160.98.30.51, 00:50:52, GigabitEthernet0/0
R     192.168.1.0/24 [120/1] via 192.168.3.1, 00:00:01, Tunnel0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/1
L        192.168.2.1/32 is directly connected, GigabitEthernet0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Tunnel0
L        192.168.3.2/32 is directly connected, Tunnel0
r2#
```

FIGURE 8 – R2

R1 :

- *160.98.0.0* est un sous-réseau contenant le LAN 1 et 4 ainsi que le PCLTE06.
- *192.168.2.0 via 192.168.3.2* est une route RIP (utilisant le tunnel GRE) qui permet d'accéder au sous-réseau de la station B depuis le sous-réseau de la station A.

R2 :

- *160.98.0.0* est un sous-réseau contenant le LAN 1 et 4 ainsi que le PCLTE06.
- *192.168.1.0 via 192.168.3.1* est une route RIP (utilisant le tunnel GRE) qui permet d'accéder au sous-réseau de la station A depuis le sous-réseau de la station B.

Problème 7

Affichez le contenu de la table de routage du routeur tlabsro04 (show ip route). Que constatez-vous ?

Table du routeur tlabsro04

```
tlablsc1016-ro04#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 160.98.30.1 to network 0.0.0.0

     160.98.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       160.98.44.128/25 is directly connected, GigabitEthernet0/0
C       160.98.30.0/23 is directly connected, GigabitEthernet0/1.30
S*   0.0.0.0/0 [1/0] via 160.98.30.1
tlablsc1016-ro04#
```

La route par défaut (*0.0.0.0/0*) est redirigée sur *160.98.30.1*.

Problème 8

Effectuez un traceroute entre la station A et la station B. Quel est le chemin emprunté ? Commentez.

Dans le cas présent, nous effectuons un traceroute depuis la station A à destination de la station B. Comme nous pouvons le remarquer, nous avons 3 entrées lors du traceroute :

- **1 - 192.168.1.1 :** Il s'agit de l'adresse IP du routeur R1.
- **2 - 192.168.3.2 :** Il s'agit de l'adresse IP du tunnel (du côté du routeur R2).
- **3 - 192.168.2.2 :** Il s'agit de l'adresse IP de la station B, elle a donc été atteinte et le traceroute est terminé

Comme nous pouvons le constater, nous n'avons que peu d'entrées lors de ce traceroute. Nous n'avons par exemple aucune adresse IP du routeur tlabsro04 or que nous sommes obligés de passer par ce noeud. Le trafic passe en effet par ce routeur, mais le tunnel VPN "masque" cette partie du réseau, il crée un lien direct virtuel entre le routeur R1 et le routeur R2.

```
MacBook-Pro-de-Samuel-2:~ samuelriedo$ traceroute 192.168.2.2
traceroute to 192.168.2.2 (192.168.2.2), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  0.994 ms  0.839 ms  0.710 ms
 2  192.168.3.2 (192.168.3.2)  1.206 ms  1.394 ms  1.023 ms
 3  192.168.2.2 (192.168.2.2)  1.256 ms  1.431 ms  1.224 ms
MacBook-Pro-de-Samuel-2:~ samuelriedo$
```

FIGURE 9 – Traceroute entre la station A et B

Problème 9

Dessinez le schéma logique de ce réseau "vu" depuis les stations A et B.

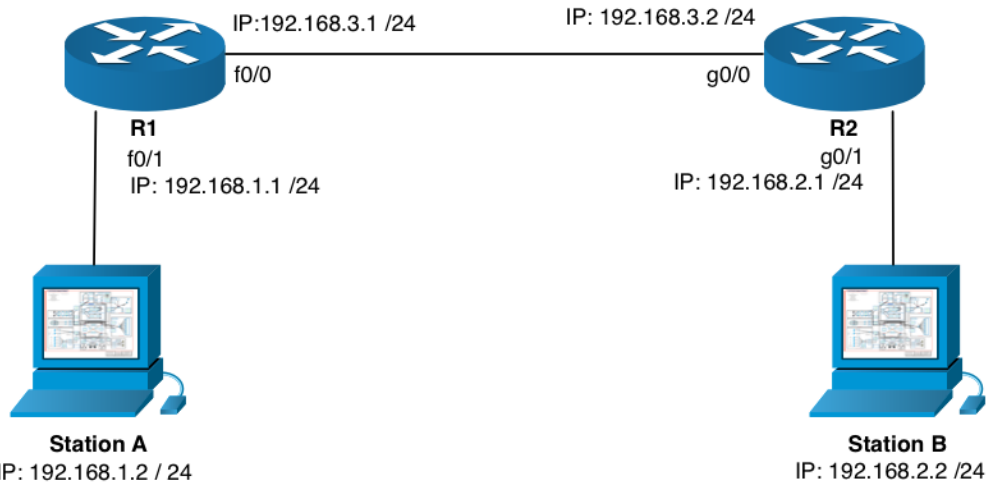

FIGURE 10 – Schéma logique vu depuis les stations A et B

Problème 10

Comment est transporté le ping entre les routeurs R1 et R2. Donnez tout le détail de votre mesure et comparez avec la RFC 2784 [2].
Le paquet ICMP est encapsulé dans un paquet GRE. Le premier est donc le payload du second. Le paquet GRE contient donc deux adresses IP.

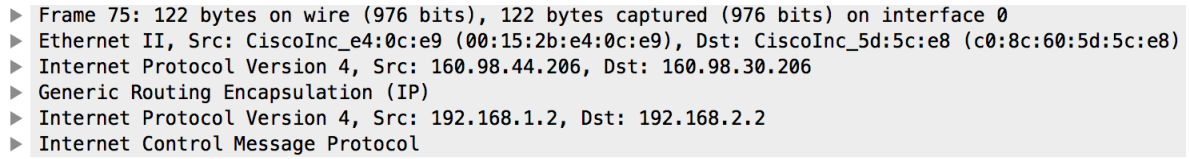

FIGURE 11 – Paquet GRE

Problème 11

Quel autre type de trafic circule au travers du tunnel ?
Dans notre cas, en plus des ping (ICMP), nous avons les informations de routages RIP qui passent dans le tunnel. Il est cependant important de remarquer que n'importe quel protocole IP pourrait s'y trouver. Il suffit, par exemple, de rediriger le trafic à l'aide d'une route par défaut utilisant une adresse du tunnel.

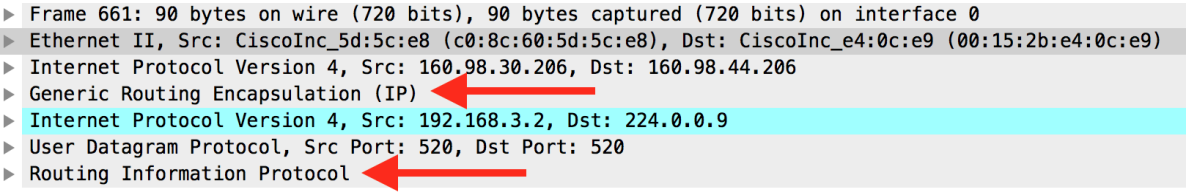

FIGURE 12 – Trame RIP passant par le tunnel VPN

Problème 12

Quelles(s) caractéristique(s) particulières (ou avantages) apporte(nt) le tunnel GRE ?
- Création d'un réseau privé sur un réseau public, sans hardware supplémentaire.
- Sépare le flux passant dans le tunnel du flux n'y passant pas par une encapsulation du paquet à transiter dans un paquet GRE.

Conclusion

Nous avons pu remarquer lors de ce TP que le VPN est un protocole très utile. Il permet en effet d'étendre un réseau privé sans exiger de matériel supplémentaire (par exemple une ligne louée).
Le VPN permet par ailleurs de masquer la topologie du réseau. En effet, si un utilisateur effectue un traceroute, il ne pourra pas voir par quels routeurs passe le tunnel (il ne verra que les routeurs d'entrée et de sortie du tunnel).

Table des figures

Fribourg, le 10 janvier 2017

Samuel Riedo

Maic Queiroz