Concept d'encapsulation : Tunnel GRE (Generic Routing Encapsulation)

Tunnel GRE (Generic Routing Encapsulation)

1. Concept d'encapsulation

Le tunnel GRE (Generic Routing Encapsulation) permet d'encapsuler un paquet (quel que soit le protocole transporté) dans un nouveau paquet IP pour traverser un réseau intermédiaire.

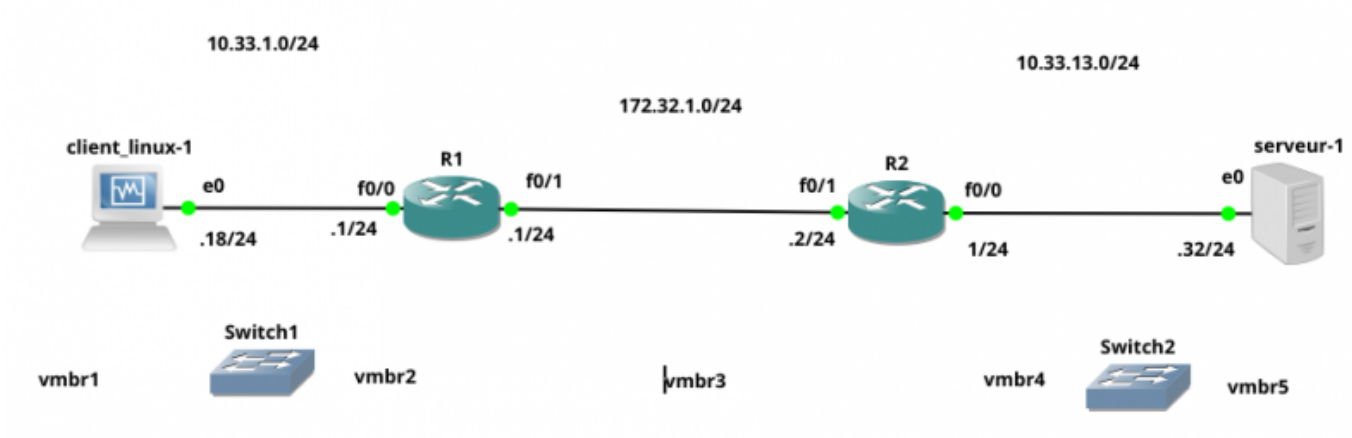
L'analogie de l'enveloppe : imaginez qu'on veuille envoyer une lettre (le paquet de l'hôte 10.33.1.18) à un ami, mais que le facteur local ne connaît pas cette adresse. On met donc la lettre dans une deuxième enveloppe avec une adresse que le facteur connaît (172.32.1.2). Une fois arrivée, notre ami ouvre la grande enveloppe et trouve la lettre originale.

Pourquoi utiliser GRE ?

- Il est `Generic` : il peut transporter presque n'importe quoi (IPv4, IPv6, paquets de routage comme OSPF/EIGRP).
- Il crée un lien direct virtuel : pour les deux routeurs, c'est comme s'ils étaient reliés par un câble invisible, même s'ils sont à 1000 km l'un de l'autre.

2. Architecture du Lab (GNS3)

Tableau d'adressage



La plateforme du LAB

Élément	Interface	Adresse IP
client_linux-1	eth0	10.33.1.18 /24 (GW: 10.33.1.1)
Router 1 (R1)	f0/0 (LAN)	10.33.1.1 /24
	f0/1 (WAN)	172.32.1.1 /24
Router 2 (R2)	f0/1 (WAN)	172.32.1.2 /24
	f0/0 (LAN)	10.33.13.1 /24
serveur-1 (PC2)	eth0	10.33.13.32 /24 (GW: 10.33.13.1)

- Image ios router C3725

3. Configuration des équipements

3.1. Configuration de R1 (Site A)

On configure d'abord les interfaces physiques, puis le tunnel.

```
! Configuration des interfaces physiques
```

```
R1(config)# interface FastEthernet0/0
R1(config-if)# ip address 10.33.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# interface FastEthernet0/1
R1(config-if)# ip address 172.32.1.1 255.255.255.0
R1(config-if)# no shutdown

! Création du Tunnel GRE
R1(config)# interface Tunnel0
R1(config-if)# ip address 192.168.100.1 255.255.255.0
R1(config-if)# tunnel source 172.32.1.1
R1(config-if)# tunnel destination 172.32.1.2

! Routage pour joindre le LAN opposé via le tunnel
R1(config)# ip route 10.33.13.0 255.255.255.0 Tunnel0
```

3.2. Configuration de R2 (Site B)

```
! Configuration des interfaces physiques
R2(config)# interface FastEthernet0/0
R2(config-if)# ip address 10.33.13.1 255.255.255.0
R2(config-if)# no shutdown

R2(config)# interface FastEthernet0/1
R2(config-if)# ip address 172.32.1.2 255.255.255.0
R2(config-if)# no shutdown

! Création du Tunnel GRE
R2(config)# interface Tunnel0
R2(config-if)# ip address 192.168.100.2 255.255.255.0
R2(config-if)# tunnel source 172.32.1.2
R2(config-if)# tunnel destination 172.32.1.1

! Routage pour joindre le LAN opposé via le tunnel
R2(config)# ip route 10.33.1.0 255.255.255.0 Tunnel0
```

4. Comprendre l’adressage du tunnel

Dans ce lab, on distingue trois niveaux d'adresses :

Type d'adresse	Réseau dans le Lab	Rôle
Adresses LAN	10.33.x.x	Les machines finales (les clients).
Adresses WAN	172.32.1.x	Le « vrai » réseau (Internet/Public).
Adresses Tunnel	192.168.100.x	L'adresse logique du lien virtuel.

À quoi sert le réseau 192.168.100.0/24 ?

1. Le routeur a besoin d'une IP sur l'interface virtuelle `Tunnel0` pour que la table de routage sache où envoyer les paquets.
2. R1 et R2 peuvent échanger des informations de routage via leurs IPs en 192.168.100.x.
3. On peut dire à R1 : « Pour aller chez l'hôte 10.33.13.32, passe par la porte 192.168.100.2 ». GRE se charge alors de l'encapsulation sur le WAN en 172.32.x.x.

5. Travail pratique

Exercice 1 : Vérification de la connectivité

Depuis l'hôte `'10.33.1.18'`, lancez un ping vers `'10.33.13.32'`.

- Question : Quel est le chemin emprunté ? (Faire un `traceroute`).

Exercice 2 : Analyse Wireshark

Lancez une capture Wireshark sur le lien entre R1 et R2 (le « WAN »).

Analyse du paquet :

1. Identifiez l`'External Header'` (IP publiques : 172.32.1.x).
2. Identifiez le protocole de tunneling (GRE - Protocol 47).
3. Identifiez l`'Internal Header'` (IP privées : 10.33.x.x).

- Question : Pourquoi voit-on le contenu en clair ? (Réponse attendue : GRE encapsule mais ne chiffre pas).

Exercice 3 : Sécurisation (ouverture vers IPsec)

Que se passerait-il si un attaquant se trouvait sur le « IPv4 Network » au milieu ?

Transition proposée : introduire IPsec en mode Transport pour chiffrer le tunnel GRE existant.

6. Analyse du « Packet Flow »

L'analyse Wireshark confirme le fonctionnement suivant :

- `Internal Header` (Rouge) : la lettre originale (Src: 10.33.1.18 → Dst: 10.33.13.32).
- `GRE Header` (Bleu) : la mention « Ceci est un tunnel ».
- `External Header` (Vert) : la grande enveloppe qui permet de voyager sur l'IPv4 Network (Src: 172.32.1.1 → Dst: 172.32.1.2).

L'adresse 192.168.100.x n'apparaît pas dans les paquets capturés sur le WAN. Elle n'existe que dans la tête des routeurs pour décider quel chemin prendre. Une fois que le routeur a décidé d'utiliser le tunnel, il remplace l'en-tête de transport par les IP WAN (172.32.x.x).

7. Conclusion

Ce TP illustre bien que le réseau est comme un oignon : on ajoute des couches.

1. GRE ajoute une couche d'adressage (tunnel logique).
2. IPsec ajoutera une couche de chiffrement par-dessus.

Résumé pour le cours : le GRE crée une illusion de proximité. L'adressage en 192.168.100.0 est la preuve de cette illusion : c'est le réseau qui connecte logiquement les deux bouts du tunnel.