

Tunnel L2 - GRETAP

1. Introduction : Pourquoi utiliser GRETAP ?

1.1. À quoi sert un tunnel GRETAP ?

Un tunnel **GRETAP (GRE Tunnel Access Point)** est une variante Layer 2 du tunnel GRE classique. Contrairement au GRE standard qui transporte des paquets IP (Layer 3), GRETAP transporte des **trames Ethernet complètes**, ce qui permet de bridger des réseaux distants comme s'ils étaient connectés au même switch. **Exemple concret :**

- Vous avez un réseau local derrière une box opérateur standard.
- Vous voulez une ou des IPs publiques directement accessibles sur vos machines, comme si elles étaient sur le même réseau que la plateforme.

1.2. Avantages de GRETAP

- Transport Layer 2 complet (trames Ethernet).
- Simple à configurer (même syntaxe que GRE classique).
- Compatible avec la plupart des équipements réseau.
- Protocole léger.
- Peut être combiné avec d'autres tunnels L2 via un bridge.

1.3. Inconvénients

- Pas de chiffrement natif.
 - Utilise le protocole 47 (comme GRE) : nécessite une redirection spécifique ou DMZ si derrière un NAT.
 - Overhead de 38 octets (en-tête GRE + en-tête Ethernet interne).
-

2. Prérequis

2.1. Ce dont vous avez besoin

- Une **IP publique** (ou une DMZ si derrière une box).
- Un **routeur ou serveur compatible GRETAP** (Linux, MikroTik, etc.).
- Un **service Tunnel-IP**.

2.2. Ports et NAT

- GRETAP utilise le **protocole 47** (comme GRE classique), ce n'est ni UDP ni TCP.
- Si le routeur final est derrière une box / NAT, il faut **rediriger le protocole GRE (47)** vers le routeur final. Certaines box ont des ALG automatiques, mais il est souvent préférable de configurer une DMZ.

3. Étape 1 : Créer le bridge et le tunnel sur Tunnel-IP.com

Les tunnels L2 fonctionnent avec des **bridges** sur la plateforme. Un bridge est un switch virtuel qui regroupe vos tunnels L2 et vos subnets. Vous devez d'abord créer un bridge, puis créer le tunnel en l'associant à ce bridge.

3.1. Créer le bridge

1. Connectez-vous à panel.tunnel-ip.com
2. Allez dans "**Bridges**".
3. Cliquez sur "**Ajouter un Bridge**" et donnez-lui un nom.
4. Validez. Le bridge sera créé sur la plateforme.

3.2. Créer le tunnel GRETAP

1. Allez dans "**Tunnels**" > "**GRETAP**".
2. Remplissez les informations :
 - **Nom du tunnel** (ex : `GRETAP_Tunnel`).
 - **Endpoint** (IP publique du routeur / box, ex : `203.0.113.1`).
 - **Bridge** : Sélectionnez le bridge créé précédemment.
 - **MTU** : Taille maximale des paquets (-1 pour laisser la plateforme choisir).
 - **Clé** (si applicable).
3. Validez. La plateforme s'occupera de configurer le tunnel côté Tunnel-IP.com.

4. Attendez que le tunnel soit créé
5. Cliquez sur "Accéder" pour récupérer les détails du tunnel

3.3. Créer le subnet

1. Allez dans "**Subnets**"
2. Copiez le bloc d'IP publique et collez le dans le formulaire
3. Sélectionnez le **bridge** (et non un tunnel directement) comme destination
4. Cliquez sur Créer
5. Une fois son statut à "Actif", la route est correctement installée sur les routeurs de la plateforme

Important : La première IP du subnet sera utilisée comme **gateway** sur le bridge côté plateforme. Par exemple, pour le subnet `198.51.100.0/29`, la gateway sera `198.51.100.1`.

4. Étape 2 : Configurer le tunnel

Contrairement au GRE classique (L3), GRE-TAP transporte des trames Ethernet (Layer 2). Côté client, vous devez créer l'interface GRE-TAP puis la **brider** avec votre interface LAN (ou lui assigner directement une IP du subnet).

4.1. Exemple pour Linux (Ubuntu/Debian)

Étapes :

1. **Créer l'interface GRE-TAP :**

```
ip link add gretap0 type gretap remote 172.16.126.33
ip link set gretap0 up
```

- `gretap0` : Nom de l'interface GRE-TAP.
- `remote 172.16.126.33` : IP distante (Tunnel-IP.com).

2. **Option A : Assigner directement une IP publique :**

Si vous souhaitez que le routeur lui-même ait une IP publique :

```
ip addr add 198.51.100.2/29 dev gretap0
ip route add default via 198.51.100.1 dev gretap0
```

- `198.51.100.2/29` : Une IP du subnet (la première IP `.1` est la gateway côté plateforme).
- `198.51.100.1` : Gateway (première IP du subnet, côté plateforme).

3. Option B : Bridger avec une interface LAN :

Si vous souhaitez que des machines sur votre LAN aient directement les IPs publiques :

```
ip link add br0 type bridge
ip link set br0 up
ip link set gretap0 master br0
ip link set eth1 master br0 # Interface LAN vers vos machines
```

Les machines connectées à `eth1` pourront alors utiliser les IPs du subnet directement, avec `198.51.100.1` comme gateway.

4. Activer le forwarding (si nécessaire) :

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

(Pour rendre permanent, ajoutez `net.ipv4.ip_forward=1` dans `/etc/sysctl.conf`*)*

4.2. Exemple pour MikroTik

MikroTik ne supporte pas nativement le GRE-TAP en tant que tel. Cependant, l'interface EoIP de MikroTik remplit la même fonction (tunnel GRE Layer 2). Si vous souhaitez interopérer avec un GRE-TAP Linux/Cisco, vous pouvez utiliser un EoIP côté MikroTik avec les mêmes paramètres, ou utiliser un bridge avec un tunnel GRE classique.

Alternative avec EoIP :

1. Créer l'interface EoIP :

```
/interface/eoip/add remote-address=172.16.126.33 tunnel-id=100 name=eoip-tunnel
```

2. Bridger avec une interface LAN :

```
/interface/bridge/add name=br-gretap
/interface/bridge/port/add bridge=br-gretap interface=eoip-tunnel
/interface/bridge/port/add bridge=br-gretap interface=ether2 # Interface LAN
```

3. Option : Assigner une IP au bridge :

```
/ip/address/add address=198.51.100.2/29 interface=br-gretap
/ip/route/add dst-address=0.0.0.0/0 gateway=198.51.100.1
```

4.3. Exemple pour Cisco (IOS/XE)

Étapes :

1. **Accéder au mode configuration :**

```
enable
configure terminal
```

2. **Créer l'interface tunnel en mode GRE :**

```
interface Tunnel0
 tunnel source 192.168.1.1 # IP locale du routeur
 tunnel destination 172.16.126.33 # IP distante
 tunnel mode gre multipoint
 no shutdown
```

3. **Créer le Bridge Domain et l'associer :**

```
bridge-domain 100
 member Tunnel0 service-instance 1
 member Vlan100
```

4. **Configurer l'interface VLAN :**

```
interface Vlan100
 ip address 198.51.100.2 255.255.255.248
 no shutdown
```

5. **Sauvegarder la configuration :**

```
write memory
```

La configuration de bridge L2 sur Cisco varie fortement selon la plateforme (IOS, IOS-XE, NX-OS). Consultez la documentation de votre modèle.

4.4. Exemple pour Arista (EOS)

Étapes :

1. **Accéder au mode configuration :**

```
enable
configure terminal
```

2. Créer l'interface tunnel GRE en mode bridge :

```
interface Tunnel0
  tunnel source 192.168.1.1
  tunnel destination 172.16.126.33
  tunnel mode gre
  no shutdown
```

3. Bridger le tunnel avec un VLAN :

```
interface Tunnel0
  switchport access vlan 100

interface Vlan100
  ip address 198.51.100.2/29
  no shutdown
```

4. Sauvegarder la configuration :

```
write memory
```

4.5. Exemple pour Juniper (JunOS)

Étapes :

1. Accéder au mode configuration :

```
edit
```

2. Créer l'interface GRE et le bridge domain :

```
set interfaces gr-0/0/0 tunnel source 192.168.1.1
set interfaces gr-0/0/0 tunnel destination 172.16.126.33
set interfaces gr-0/0/0 family bridge interface-mode trunk
set interfaces gr-0/0/0 family bridge vlan-id-list 100

set bridge-domains GRETAP-BD vlan-id 100
set bridge-domains GRETAP-BD routing-interface irb.100
```

```
set interfaces irb unit 100 family inet address 198.51.100.2/29
```

3. Appliquer la configuration :

```
commit
```

5. Étape 3 : Configurer les IPs publiques

5.1. Architecture L2

```
Internet → [Infrastructure Tunnel-IP.com] → [Bridge plateforme] → (Tunnel GRE/TAP) → [Votre Bridge/Interface] → [Vos Machines]
```

- La plateforme met la première IP du subnet comme gateway sur le bridge (ex: `198.51.100.1`).
- Vos machines utilisent les autres IPs du subnet.
- Comme le tunnel est L2, les trames Ethernet passent directement, **pas besoin de NAT ni de routage complexe**.

5.2. Attribution des IPs

Un `/29` contient **8 adresses IP** :

- `198.51.100.0` : Adresse réseau (inutilisable).
- `198.51.100.1` : **Gateway plateforme** (réservée automatiquement).
- `198.51.100.2` à `198.51.100.6` : IPs utilisables pour vos machines.
- `198.51.100.7` : Adresse broadcast (inutilisable).

5.3. Configuration sur les machines

Sur chaque machine qui doit utiliser une IP publique :

Linux :

```
ip addr add 198.51.100.2/29 dev eth0  
ip route add default via 198.51.100.1
```

MikroTik :

```
/ip/address/add address=198.51.100.2/29 interface=ether1  
/ip/route/add dst-address=0.0.0.0/0 gateway=198.51.100.1
```

Si vous avez bridgé l'interface GREYAP avec votre LAN, les machines peuvent être configurées directement avec les IPs publiques et la gateway `198.51.100.1`, comme si elles étaient sur un réseau local classique.

6. Commandes spécifiques par constructeur

Constructeur	Commande pour vérifier le tunnel	Commande pour vérifier le bridge
Linux	<code>ip -d link show gretap0</code>	<code>bridge link show</code>
MikroTik	<code>/interface eoip print</code>	<code>/interface bridge port print</code>
Cisco	<code>show interface Tunnel0</code>	<code>show bridge-domain</code>
Arista	<code>show interface Tunnel0</code>	<code>show vlan</code>
Juniper	<code>show interfaces gr-0/0/0</code>	<code>show bridge-domain</code>

7. Vérification et Dépannage

7.1. Tester la connectivité

- Depuis votre routeur / machine :

```
ping 198.51.100.1 # Ping de la gateway plateforme
```

- Vérifier l'interface GREYAP (Linux) :

```
ip -d link show gretap0 # Vérifier les paramètres  
bridge fdb show dev gretap0 # Vérifier la table MAC
```

- Depuis une machine locale :

```
ping 8.8.8.8 # Vérification internet
curl -4 ifconfig.me # Vérification de l'IP sortante
```

7.2. Problèmes courants

Symptôme	Cause Possible	Solution
Le tunnel ne répond pas	Protocole 47 bloqué	Vérifiez la redirection sur votre box / configurez une DMZ
Pas de connectivité L2	Clé GRE incorrecte	Vérifiez que la clé correspond à celle fournie par la plateforme
La gateway ne répond pas	Subnet non associé au bridge	Vérifiez que le subnet est bien associé au bridge sur la plateforme
Latence élevée / Pertes de paquets	MTU trop grande	Réduisez la MTU : <code>ip link set mtu 1462 dev gretap0</code> (overhead GRE-TAP = 38 octets)
Les IPs publiques ne fonctionnent pas	Mauvaise gateway	Utilisez la première IP du subnet comme gateway (ex: <code>198.51.100.1</code>)

8. Bonnes Pratiques

1. Sécurité :

- Filtrez le trafic entrant avec un pare-feu (ex: `iptables` ou ACL).
- GRE-TAP n'offre aucun chiffrement natif. Envisagez IPsec ou Wireguard en complément si le chiffrement est nécessaire.

2. Performance :

- Réduisez la MTU à `1462` pour éviter la fragmentation (overhead GRE-TAP = 38 octets).
- Vérifiez que la MTU de votre lien WAN est suffisante pour encapsuler les trames.

3. Bridging :

- Vous pouvez combiner plusieurs tunnels L2 (VXLAN, EoIP, GRE-TAP) sur le même bridge, aussi bien sur la plateforme que côté client.
- Attention aux boucles de bridge : activez le STP si nécessaire.

Revision #4

Created 2026-03-30 14:29:10 UTC by Landry JUGE

Updated 2026-03-30 14:41:41 UTC by Landry JUGE