

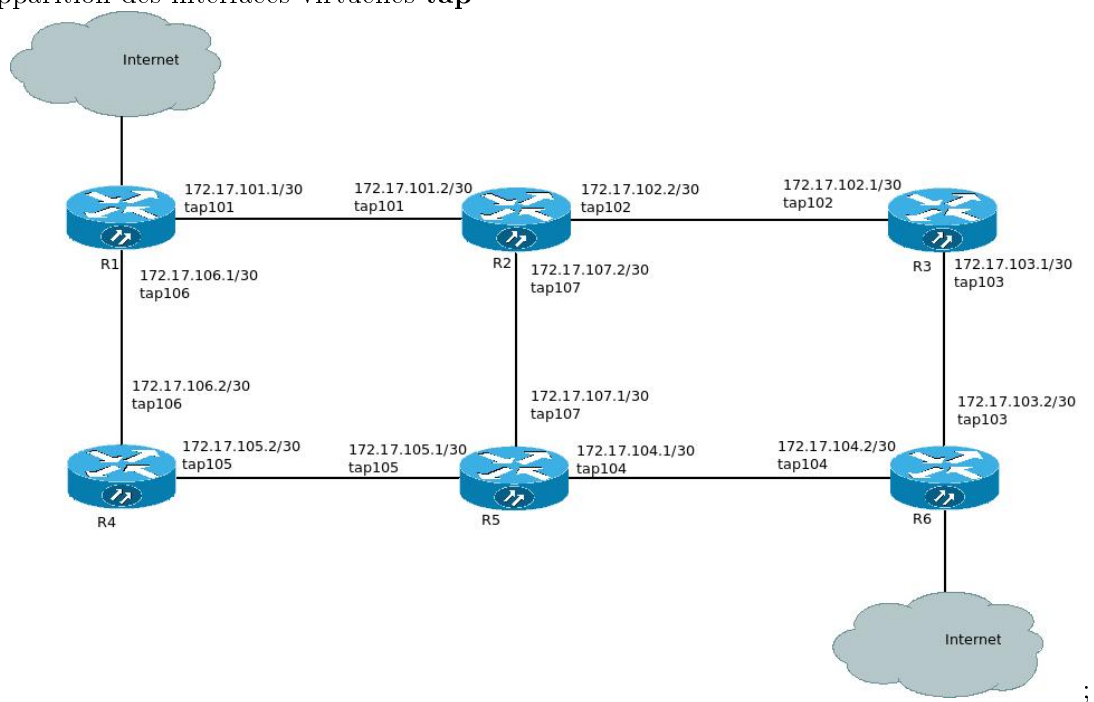
LANL - TP06

1 Introduction

Ce TP est consacré à la mise en place d'un LAN routé virtuel en utilisant des tunnels VPN. Nous allons utiliser le logiciel Tinc VPN <https://www.tinc-vpn.org/>

Nous allons remonter la même topologie que le TP précédent mais au lieu d'utiliser des liaisons physiques avec des vlan, nous utiliserons les tunnels VPN.

Nous allons donc construire la topologie suivante. la seule différence est l'apparition des interfaces virtuelles **tap**



2 Tinc : fonctionnement et mise en application

Le logiciel *tinc* fonctionne sur base de clef asymétriques. Un serveur donné possède un couple clef privée/clef publique. La clef privée ne quitte

jamais le serveur (en théorie) et la clef publique est communiquée aux autres serveurs avec lesquels on souhaite établir un tunnel.

L'établissement d'un tunnel vpn *tinc* entre serveurs revient donc communiquer les clefs publiques entre ces serveurs.

Dans un réseau tinc configuré en mode *Switch* (layer-2), plusieurs serveurs peuvent apparaître, il s'agit donc d'un switch virtuel.

Afin de simuler les liaisons physiques du dernier TP, nous allons créer plusieurs réseaux *tinc* dans lesquels apparaissent au maximum deux serveurs : liaisons point à point.

Un serveur donné devra donc tourner plusieurs démons *tinc* (un par liaison). ces démons feront chacun apparaître au système d'exploitation une interface virtuelle.

Nous allons utiliser la numérotation des VLAN attribués au dernier TP pour nommer les interfaces virtuelles et les numéros de ports. Pour ces derniers, nous utiliserons les ports compris entre 33000 et 33999.

Par exemple, le routeur **R1** est connecté aux routeurs **R2** et **R4**. Il tournera donc deux démons tinc :

- un pour la liaison vers *R2* en utilisant les ports TCP et UDP **33101** et faisant apparaître l'interface virtuelle **tap101**
- un pour la liaison vers *R4* en utilisant les ports TCP et UDP **33106** et faisant apparaître l'interface virtuelle **tap106**

3 Configuration

La configuration d'un démon tinc consiste donc à définir les quelques options suivantes :

- le nom du démon
- les numéros de port sur lesquels écouter
- le nom de l'interface virtuelle à créer
- les autres serveurs auxquels se connecter ainsi que leur clef publique respective

Pour éviter de passer tout le temps de la séance à s'échanger les clefs publiques, la configuration de tous les démons a été prévue à l'avance et il vous est juste demandé de télécharger la configuration de votre routeur, de renseigner les adresses IP et faire le debugging.

Le logiciel place sa configuration dans le répertoire */etc/tinc* dans lequel on trouve un répertoire par démon. Par exemple, sur le routeur *R1* le démon chargé du tunnel vers *R2* sera placé dans le répertoire */etc/tinc/r1r2*.

3.1 Instructions

- installez le paquet *tinc*
- placez vous dans le répertoire */etc/tinc/*

- téléchargez **les** configurations qui vous correspondent, par exemple pour *R6*
 - `wget http://debian.jsnet.be/tinc/r6r3.tar.gz`
 - `wget http://debian.jsnet.be/tinc/r6r5.tar.gz`
- décompressez les archives :
 - `tar -zxvf r6r3.tar.gz`
 - `tar -zxvf r6r5.tar.gz`
- dans chaque dossiers vous avez toute la configuration nécessaire pour établir le tunnel concerné
- renseignez juste les adresse ip de votre serveur et du serveur distant dans les fichiers du sous-dossier *hosts/*

4 Démarrage et diagnostic

Comme tout logiciel, *Tinc* peut être démarré en arrière plan (background) ou en avant plan (foreground) à des fins de debug.

- Démarrage en avant plan : `tincd -D -d 5 -n <name>` ou `<name>` est le nom du répertoire, exemple *r2r1*
- Démarrage en arrière plan : `systemctl start tinc; systemctl status -l tinc`

Une fois démarré, vous les interfaces virtuelles devraient apparaitre. Configurez les adresse ip correspondantes, et lancer le démon OSPF en lui indiquant bien les bonnes interfaces.