Travaux Pratiques
Routage statique avancé (IOS)
et avec filtrage (pare-feu)

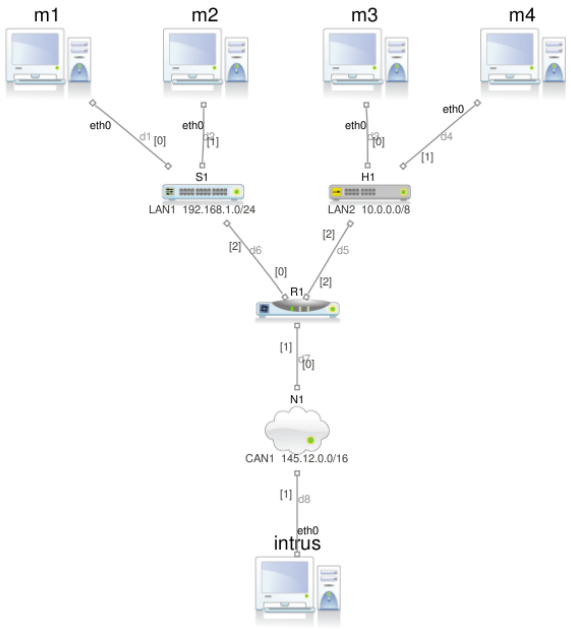
Séance de TP entièrement effectuée avec le logiciel Marionnet. Durée estimée : 2h - 2h30.

Prérequis. Avoir compris les notions de routage (1ère partie) et de filtrage (2ème partie), et leur mise en oeuvre sous GNU/Linux avec iptables.

Câblage et configuration du réseau local

Deux machines, m_1 et m_2 et un commutateur S_1 réalisent un réseau local $LAN_1 = \{m_1, m_2\}$ en 192.168.1.0/24. Deux autres machines m_3 et m_4 et un concentrateur H_1 réalisent un réseau local $LAN_2 = \{m_3, m_4\}$ en 10.0.0.0/8. Un troisième réseau CAN_1 (Campus Area Network) sera constitué d'une machine appelée *intrus* et d'une partie indéfinie (de niveau 2) représentée par le composant marionnet "nuage". Un routeur assurera la laison (de niveau 3) entre LAN_1 (port 0), LAN_2 (port 2) et CAN_1 (port 1).

Distributions GNU/Linux. Utilisez n'importe quelle distribution : il suffira de pouvoir lancer les commandes basiques de configuration et observation du réseau (`ifconfig`, `route`, `tcpdump`, ...)

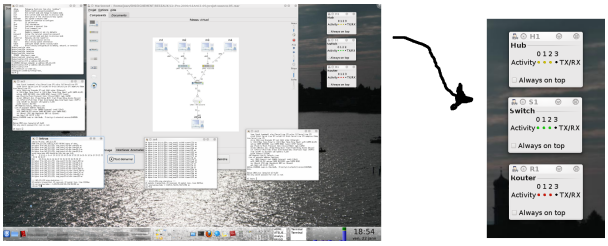


Attribution des IP. Par simplicité, la machine m_i aura l'adresse 192.168.1.i ou 10.0.0.i selon le réseau d'appartenance. Le routeur R_1 doit avoir son port 0 branché au LAN_1 et configuré en 192.168.1.254 (cela se fait dans la fenêtre de dialogue à l'ajout du routeur ou à travers l'onglet *Interfaces* de Marionnet). Concernant le réseau CAN_1, la machine *intrus* prendra le 145.12.0.42, et le routeur prendra le 145.12.0.53 sur le port 1 (`eth1`).

Première partie
Routage avancé (CISCO IOS "like")

Le but du TP est, dans cette première partie, de faire communiquer l'ensemble des réseaux définis.

Astuce. Il est fortement conseillé d'observer les petites fenêtres graphiques représentant les appareils de concentration (H_1), commutation (S_1) et routage (R_1). Cela permet de vérifier facilement où se situe un problème de non acheminement de paquets ou trames. Pour garder constamment une vision, et donc un contrôle, de l'état des liaisons, vous pouvez réduire la fenêtre principale de Marionnet de façon à laisser la place, sur un côté de l'écran, aux 3 fenêtre correspondantes aux appareils :



Commencez par tester la réponse du routeur à un ping (ECHO REQUEST du protocole ICMP) provenant d'une machine du LAN_1. Lorsque ce ping fonctionne, vous pouvez vous connecter en telnet au routeur avec le mot de passe *zebra* :

```
m1~#  telnet 192.168.1.254 2601
```

À ce stade, vous êtes connecté et vous pouvez commencer la configuration du routeur grâce à l'interpréteur de commandes IOS CISCO (que le démon du logiciel *quagga*, avec lequel vous êtes connecté, simule). La première commande à taper est celle qui permet de passer en mode administration :

```
Router> enable
Password: zebra
Router#
```

Habituez-vous à utiliser la touche *point d'interrogation* ? pour demander la complétion de vos commandes à l'interpréteur. Par exemple, avec :

```
Router# configure ?
  terminal  Configuration terminal
```

vous aurez appris de pouvoir écrire la commande :

```
Router# configure terminal
Router(config)#
```

Essayez donc seuls, avec l'aide de la touche ?, de trouver la séquence de commandes pour :
- configurer l'interface `eth2` (LAN2) en 10.255.255.254
- configurer l'interface `eth1` (CAN1) en 145.12.0.53

Puis, pour que la configuration soit persistante, pensez à faire :

```
Router(config-if)# write memory
Configuration saved to /etc/quagga/zebra.conf
```

Vous devez pouvoir tester votre configuration (effectuée donc par l'interpréteur IOS) depuis les autres machines :

```
m4~#  ping 10.255.255.254
intrus~#  ping 145.12.0.53
```

En modifiant les tables de routage de chaque machine, assurez-vous que **toutes les machines puissent communiquer entre elles** (de n'importe quel réseau à n'importe quel autre). Il est conseillé de modifier tous les fichiers `/etc/hosts` de façon à faire les tests avec des noms de machine symboliques.

Deuxième partie

Filtrage

Remplacez le routeur $R1$ par une machine GNU/Linux, appelée *router*, rendant, tout au moins initialement, **le même service** que $R1$. Quand vous aurez terminé ce remplacement, c'est-à-dire quand toutes le machines pourront à nouveau communiquer entre elles, faites en sorte que *intrus* (l'extérieur de l'organisation) ne puisse plus communiquer avec le LAN_1 ni avec le LAN_2, mais que LAN_1 et LAN_2 (l'intérieur de l'organisation) puissent continuer à communiquer. Et quand vous aurez obtenu ce résultat, réfléchissez à la question : comment faire en sorte que personne puisse "rentrer" tout en permettant aux machines du LAN_1 et LAN_2 de "sortir" sur d'autres réseaux ? (la réponse est dans les mots clef `state`, `NEW`, `ESTABLISHED`, `RELATED` que vous pouvez chercher dans le manuel de la commande `iptables`).