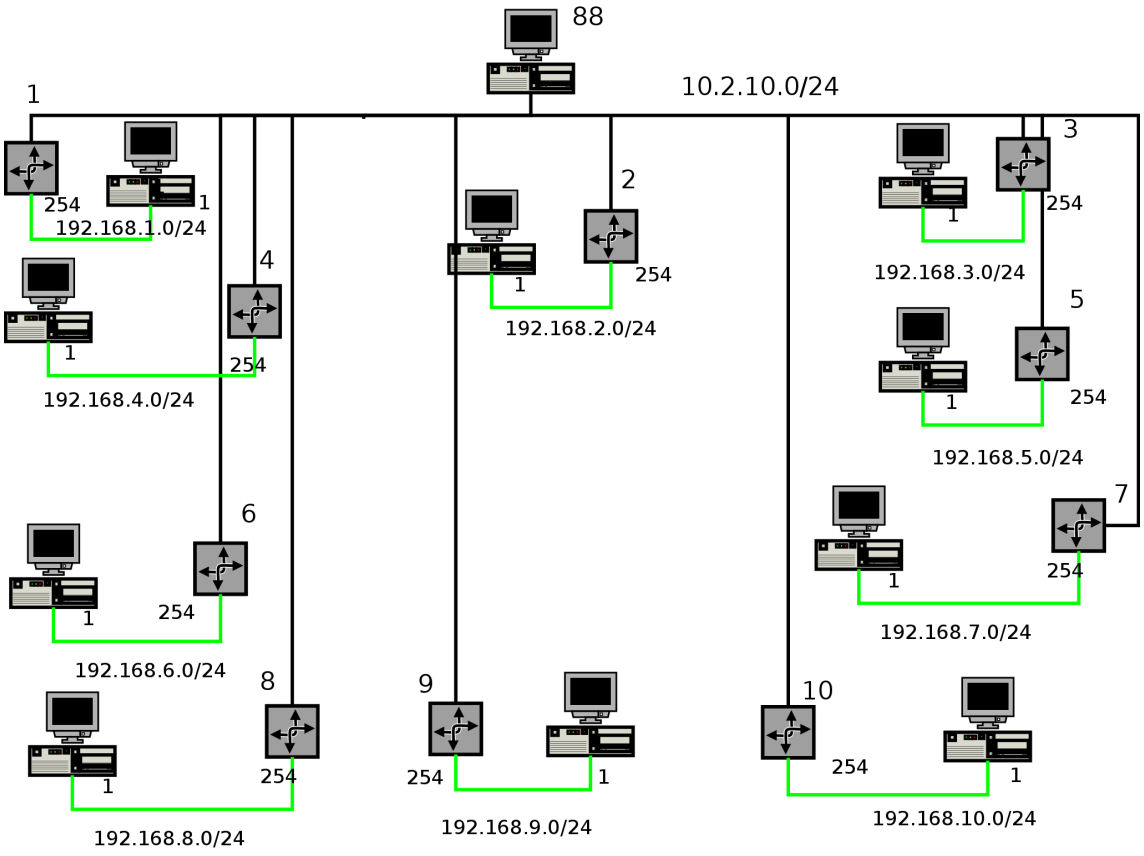
TP Netfilter

1 préambule

Au cours de ce TP vous utiliserez la configuration réalisée lors du TP routage. Le vocable "routeur" désignera la machine pourvue de 2 interface et "poste de travail" celle qui n'en a qu'une. Les tests "venant de l'extérieur" seront exécutés à partir de la machine "enseignant.tp.org".
Vous capturerez les trames qui transitent par le routeur en lançant 2 instances d'ethereal. Une pour eth0 et l'autre pour eth1.
Au cours de ce TP, vous réaliserez le réseau ci dessous :



Le plus important dans ce TP est de définir une procédure de tests pour chaque exercice. Des tests inappropriés ou insuffisants peuvent vous faire croire que vous avez obtenu le résultat attendu alors qu'il n'en est rien.

2 Exercice 1 : ping

Le poste de travail ne peut que "pinguer" les machines du backbone et des autres réseaux. Il peut être "pingué" lui-même.

1. Effacez toutes les règles qui pourraient exister
2. Définissez vos stratégies par défaut (vous les conserverez pendant tout le TP)
3. Écrivez les règles correspondantes
4. Testez

3 Exercice 2 : surf

Le poste de travail peut seulement surfer sur le web

1. Effacez les règles précédentes
2. Écrivez les règles correspondantes
3. Testez

4 Exercice 3 : serveur

Maintenant le poste de travail devient serveur web exclusivement pour le backbone mais aussi ssh pour le réseau interne. Le poste de travail n'est plus un client.

1. Effacez les règles précédentes
2. Vérifiez que l'on peut se connecter sur le poste de travail par ssh
3. Vérifiez que l'on peut se connecter sur le poste de travail sur un serveur web (au besoin installez-le)
4. Ecrivez les règles correspondantes
5. Testez

5 Exercice 4 : masquerading (NAT)

Vous allez maintenant masquer les adresses IP de notre réseau local. Deux raisons pour cela :

1. Votre FAI ne vous donne (loue ?) qu'une seule adresse IP et vous avez tout un réseau à connecter à Internet. Utilisez dans ce cas un adressage "privé" pour votre réseau local.
2. Vous voulez cacher le réseau local au reste du monde.
3. Utilisez la chaîne POSTROUTING, qui s'applique après la décision de routage.
4. Faites des captures sur toutes les interfaces et expliquez ce qui se passe.
5. Maintenant, renvoyez les demandes de connexion externes (ssh) sur le port 1234 TCP vers le poste de travail (port 22 TCP).

6 Exercice 5 : prévenir le "Deny of Service"

Le DoS est une attaque qui consiste à noyer une machine sous une avalanche de paquets dans le but de la mettre à genoux. Une parade est de limiter certains trafic. Essayez de limiter les "ping".

7 Exercice 6 : "logger"

Enregistrez dans le journal les pings reçus de la station de travail (le journal est dans /var/log/message, vous le visualisez facilement avec tail ou mieux tail -f). Vous pouvez limiter la fréquence.