

# Julien Iguchi-Cartigny

## Associate Professor, XLIM, University of Limoges, France

- [View](#)
- [Edit](#)
- [History](#)
- [Print](#)

[Netkit](#) » DMZ

- [Netkit Menu](#)
  
- [Installation](#)
- [Support sniffing](#)
- [FAQ](#)

Labs

- [Lab 1: Introduction](#)
- [Lab 2: Routage IP](#)
- [Lab 3: Lan](#)
- [Lab 4: Firewall](#)
- [Lab 5: VLAN](#)
- [Lab 6: Isolation](#)
- [Lab 7: STP](#)
- [Lab 8: Tunnel](#)
- [Lab 9: VPN](#)

[Back to Homepage](#)

Vous pouvez rectifier / améliorer cette page en vous connectant avec vos identifiants ENT de l'université de Limoges.

## Isolation des éléments d'un réseau local

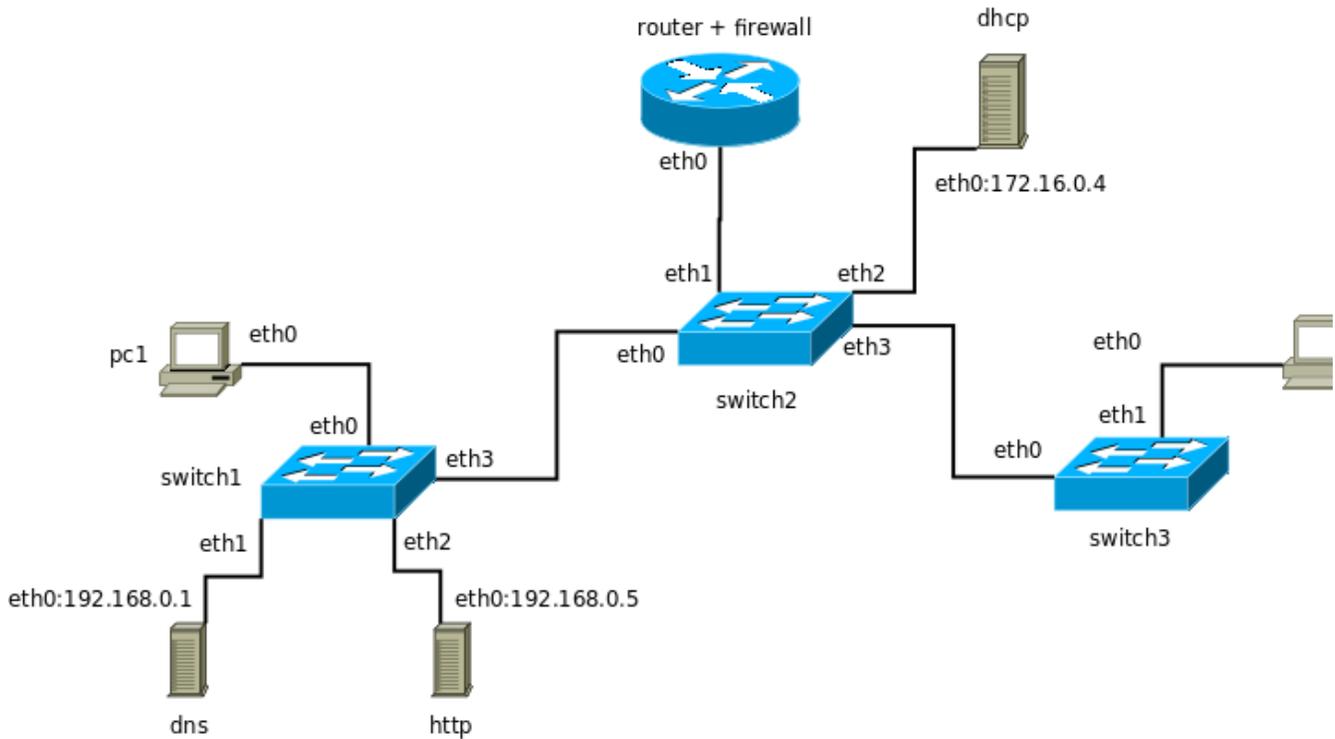
Ce TP a pour but de résumer les notions vus dans les précédentes parties.

### Scénario

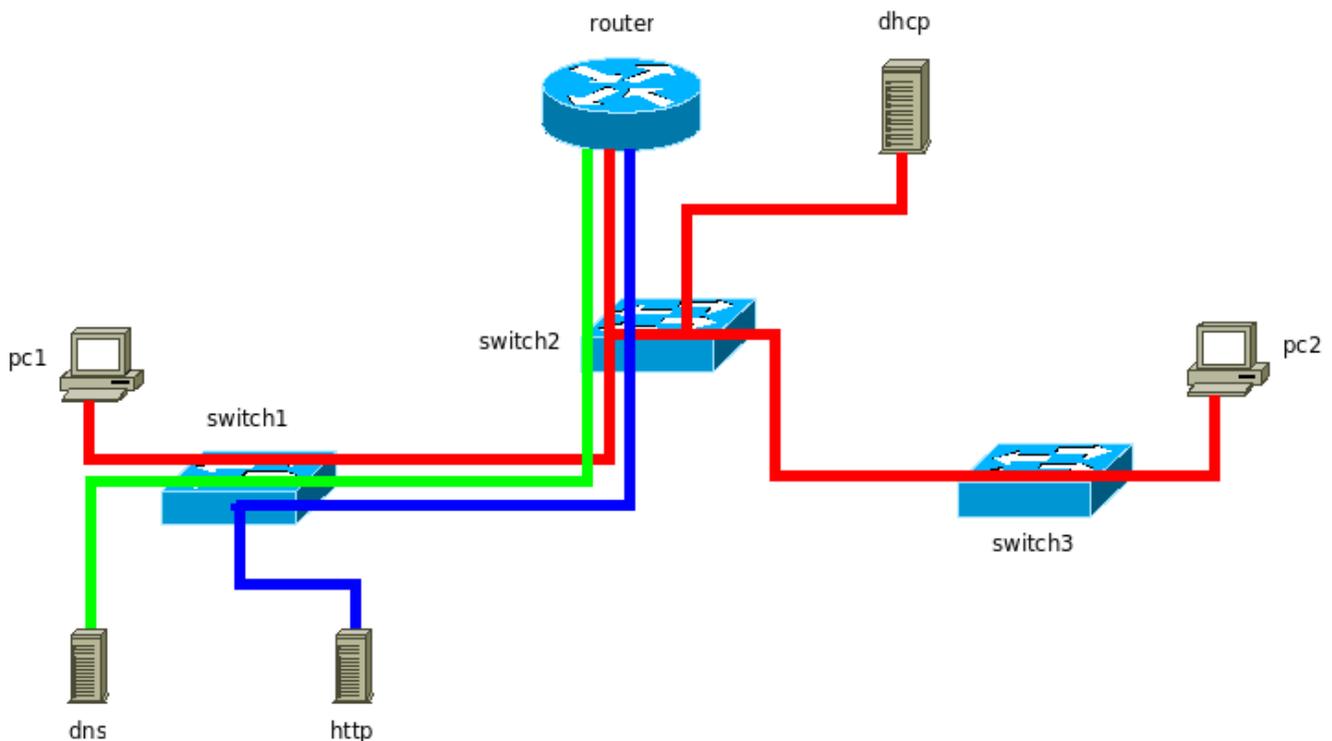
Installer et démarrer le tp (aussi disponible [ici](#)):

```
host> tar xvzf /home/shares/cartigny_softs/works/netkit/dmz.tgz -C /tmp/  
host> cd /tmp/dmz/  
host> lstart -p
```

Nous désirons configurer le scénario suivant:



L'organisation logique (des VLANs) est la suivante:



En ce qui concerne les machines:

- \* pc1 et pc2: deux clients, configuré par le serveur DHCP
- \* dns: fourni le service DNS
- \* http: possède un serveur web
- \* dhcp: fourni le service dhcp pour pc1 et pc2
- \* routeur: route les messages entre sous-réseaux

Les adresses IPs indiqués sur le plan sont déjà configurés.

Le firewall devra établir une **DMZ** autour de dns et http, c'est-à-dire que dns et http peuvent seulement répondre à des demandes concernant leur service (dns et http donc). Ils ne doivent en aucun cas pouvoir initier eux-même une communication, ni pouvoir recevoir d'autres demandes de connexion: ils sont isolés pour limiter les risques d'attaques sur eux mais aussi empêcher qu'ils puissent déborder sur le réseau s'ils sont corrompus.

Configurer les machines et vérifier qu'elles fonctionnent correctement.

© Copyright 2006-2009 - by Julien Iguchi-Cartigny

Design based on [AdSenseReady CSS](#) by [Luka Cvrk](#) ; [David Herreman](#) ; [Minimalistic Design](#)