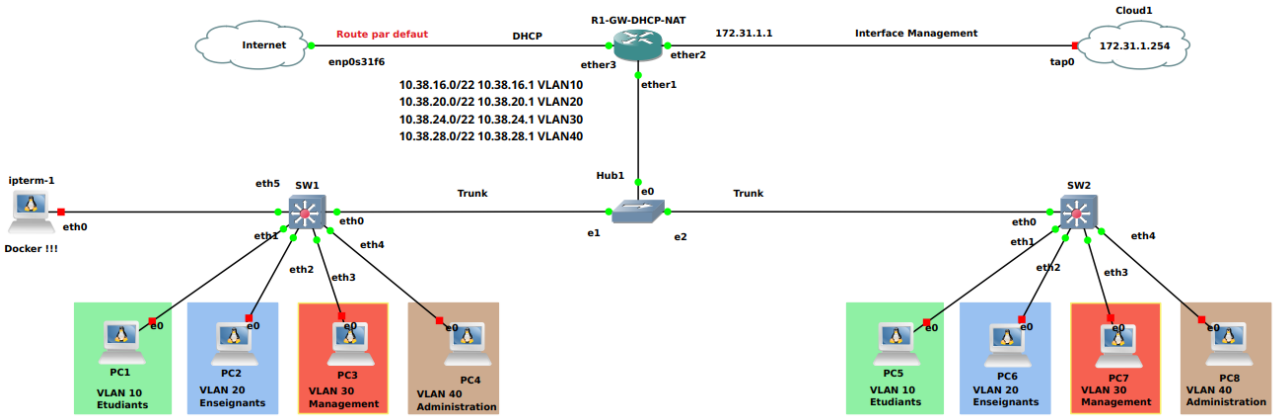
UNIVERSITÉ CAEN NORMANDIE

TP VLAN-2

07.02.2023

Auteur : Pascal Fougeray



Source : Moi ☺

1 Préambule

- **Ce TP peut être fait chez vous**, il s'appuie sur le TD intitulé Switch & Vlan ☺
- On travaille dans la VM et qu'avec les logiciels GNS3 et Wireshark
- Vous devez vous rappeler ce qu'est un
  - **vlan**
  - **une interface physique ou virtuelle !**
  - **Le routage Inter Vlan**
  - **Le filtrage pour la sécurité**
- **Prenez des notes sur ce que vous comprenez, ces notes vous y aurez le droit de les avoir avec vous au CT !**

2 Introduction

Dans ce TP, je vous propose de **voir** et **revoir** :

- Les vlan
- Les interfaces virtuelles (vlan)
- Le principe des vlan par port et surtout leur intérêt !
- Un début de routage malgré que le cours ne soit pas encore fait
- etc...

3 L'étude théorique

Voici le conf du routeur

```
/system identity name=Passerelle-DHCPServeur-FireWall
/ip dhcp-client remove 0
/interface bridge add name=lo
/interface vlan
```

```
  add interface=ether1 name=vlan10 vlan-id=10
  add interface=ether1 name=vlan20 vlan-id=20
  add interface=ether1 name=vlan30 vlan-id=30
  add interface=ether1 name=vlan40 vlan-id=40
/ip address
  add address=1.1.1.1 interface=lo network=1.1.1.1
  add address=172.31.1.1/24 interface=ether2 network=172.31.1.0
  add address=10.38.16.1/22 comment="VLAN Etudiants" interface=vlan10 network=10.38.16.0
  add address=10.38.20.1/22 comment="VLAN Enseignants" interface=vlan20 network=10.38.20.0
  add address=10.38.24.1/22 comment="VLAN Administration" interface=vlan30 network=10.38.24.0
  add address=10.38.28.1/22 comment="VLAN DSI" interface=vlan40 network=10.38.28.0
/ip pool
  add name=Etudiants ranges=10.38.16.10-10.38.19.254
  add name=Enseigants ranges=10.38.20.10-10.38.23.254
  add name=Management ranges=10.38.24.10-10.38.27.254
  add name=Administration ranges=10.38.28.10-10.38.31.254
/ip dhcp-server
  add address-pool=Etudiants disabled=no interface=vlan10 lease-time=1d name=Etudiants
  add address-pool=Enseigants disabled=no interface=vlan20 lease-time=1d name=Enseignants
  add address-pool=Administration disabled=no interface=vlan30 lease-time=1d name=Management
  add address-pool=DSI disabled=no interface=vlan40 lease-time=1d name=Administration
/ip dhcp-server network
  add address=10.38.16.0/22 dns-none=yes gateway=10.38.16.1
  add address=10.38.20.0/22 dns-none=yes gateway=10.38.20.1
  add address=10.38.24.0/22 dns-none=yes gateway=10.38.24.1
  add address=10.38.28.0/22 dns-none=yes gateway=10.38.28.1
/ip firewall nat add action=masquerade chain=srcnat out-interface=ether2
/ip route add distance=1 gateway=ether2
```

1. Que peut-on en déduire ?
   (a) Combien d'interfaces physiques a ce routeur ?
   (b) Combien d'interfaces virtuelles ou sous-interfaces a ce routeur ?
2. Quelles sont le fonctions qu'ils réalisent ?
   (a) Est-il passerelle ?
   (b) Est-il client DHCP ?
   (c) Est-il serveur DHCP ?
   (d) Est-il serveur DNS ?
   voir les lignes
   /ip dhcp-server network add address=10.38.16.0/22 **dns-none=yes** gateway=10.38.16.1
3. Que fait la ligne : ***/ip firewall nat add action=masquerade chain=srcnat out-interface=ether2*** ?
4. Que fait la ligne : ***/ip pool add name=Etudiants ranges=10.38.16.10-10.38.19.254*** ?
5. Que fait la ligne : ***/ip dhcp-server network add address=10.38.16.0/22 dns-none=yes gateway=10.38.16.1*** ?

   Nous avons déjà fait cela au TP Vlan-1
6. PC1 et PC5 sont dans le même Vlan, peuvent-ils communiquer ?
7. PC1 et PC2 sont dans 2 Vlans différents, peuvent-ils communiquer ?
8. Que faudrait-il faire pour qu'ils puissent communiquer ?

4 L'étude pratique

4.1 Partie routage inter vlan

Normalement tout est configuré ! ! !

1. **Lancez** en premier le routeur et les 2 switchs attendre 30s voire 1mn en répondant à la question suivante
2. Pourquoi est-ce que je vous demande de procéder comme cela ? Le temps de répondre les routeurs et les 2 swichs devraient avoir démarrés
3. **Lancez** les 8 PC micro-linux attendre 30s voire 1mn tout en lisant les questions suivantes
4. **Mettez** 2 sondes wireshark, avec les filtres **arp || icmp**
   (a) une sur un des 2 liens **Trunk**
   (b) une entre le **hub** et le **routeur**
5. **Relevez** l'@IP de PC1 et de PC5, sont-ils dans le même réseau ?
6. **Faites** un ping de PC1 et de PC5,
   (a) Combien de trames **arp** a-t'on ?
   (b) Quel est la valeur de **l'ID du Vlan** ? Est-ce logique ?
   (c) Par où passe la trame arp et le paquet icmp ?
7. **Faites** un traceroute de PC1 vers PC5 pour vérifier votre réponse à la question précédente
8. **Relevez** l'@IP de PC1 et de PC2, sont-ils dans le même réseau ?
9. **Faites** un ping de PC1 et de PC2,
   (a) combien de trames **arp** a-t'on ?
   (b) Quel est la valeur de **l'ID du Vlan** ? Est-ce logique ?
   (c) Par où passe la trame arp et le paquet icmp ? Commande traceroute ☺
10. **Concluez** sur le routage Inter Vlan

4.2 Partie sécurité

On veut faire en sorte que les Vlans puissent communiquer dans un sens mais pas dans l'autre

1. **Loguez** vous sur le routeurs : admin et sans MDP !
2. **Lancez** les commandes suivantes
   (a) ***ip dhcp-server lease print***
   (b) ***ip dhcp-server network print***
   (c) ***ip dhcp-server print***
3. **Expliquez** ce que vous comprenez

   On va modifier la configuration du routeur
   Si on veut filtrer et faire que seul VLAN 40 Administration puisse aller dans les VLAN 10,20 et 30 mais pas l'inverse
4. **Saisissez** les 10 lignes de configuration suivante sur le routeur.
   Un copier-coller doit fonctionner ☺

```
/ip firewall filter add action=accept chain=forward comment="accept established"
        connection-state=established

/ip firewall filter add action=drop chain=forward in-interface=vlan10 out-interface=vlan20
/ip firewall filter add action=drop chain=forward in-interface=vlan10 out-interface=vlan30
/ip firewall filter add action=drop chain=forward in-interface=vlan10 out-interface=vlan40

/ip firewall filter add action=drop chain=forward in-interface=vlan20 out-interface=vlan10
/ip firewall filter add action=drop chain=forward in-interface=vlan20 out-interface=vlan30
/ip firewall filter add action=drop chain=forward in-interface=vlan20 out-interface=vlan40

/ip firewall filter add action=drop chain=forward in-interface=vlan30 out-interface=vlan10
/ip firewall filter add action=drop chain=forward in-interface=vlan30 out-interface=vlan20
/ip firewall filter add action=drop chain=forward in-interface=vlan30 out-interface=vlan40
```

5. **Vérifiez** que seuls PC4 et PC8 peuvent pinguer les autres !
6. **Concluez** sur ce mécanisme de sécurité

4.3 Partie un peu plus loin ☺

Pour ceux qui veulent, vous pouvez ajouter deux nouveaux Vlans

1. Un Vlan nommé **serveurs** où tout le monde à accès mais pas des Serveurs aux Autres
   (a) un /28 devrait suffire
2. Un Vlan nommé **invité** qui n'a accès qu'à Internet
   (a) un /24 devrait suffire

5 Conclusion

Les Vlans ç'est utile ? Non ?