UNIVERSITÉ CAEN NORMANDIE

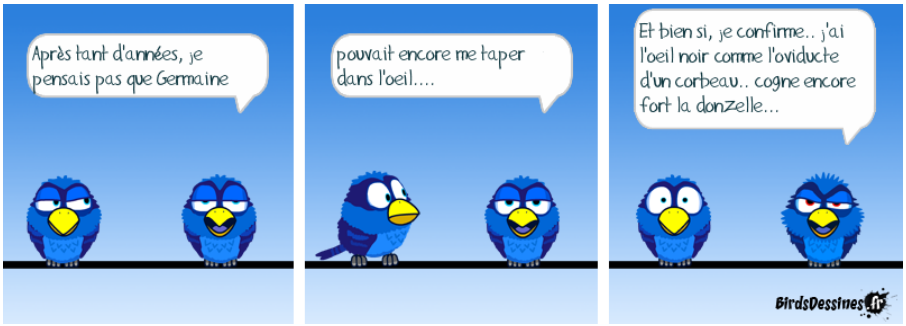
# Switch & VLAN 30.01.2023

***Onomatopée indiquant un bruit soudain ☺***

## *Et vlan passe moi l'IP...*

---

Auteur : Pascal Fougeray




source : https://www.birdsdessines.fr/2014/01/17/et-vlan-13/

---

# 1 Introduction

Voici la phrase à retenir !

Grâce à la technologie des ***réseaux locaux virtuels*** (**VLAN *Virtual Local Area Network***), les architectes réseau peuvent **segmenter** les périphériques physiques en **sous-groupes logiques** et bénéficier d'avantages en matière de **performance** et de **sécurité**.

Les VLAN (***Virtual Lan***)fonctionnent soit au niveau de
— la couche de liaison de données, couche 2,
— la couche réseau, couche 3,
en fonction de la conception du réseau.

**Les vlans ne peuvent pas communiquer entre eux à moins que l'on utilise un routeur !**

Pour faire des VLAN il suffit de posséder un **switch** *ou* **commutateur réseau paramétrable** ou dit ***"manageable"*** !

# 2 Le switch

**Il ne travaille que sur la couche 2 du modèle OSI**

Lorsque plusieurs postes de travail sont reliés en réseau au sein du même parc informatique, on utilise un **switch**, ou **commutateur réseau** qui reçoit et répartit les différentes informations sur le réseau informatique.

Cela permet d'améliorer les performances du réseau en consommant moins de bande passante.

De plus, il contribue à la protection des données informatiques et régulant l'accès aux informations échangées.

## 2.1 C'est quoi ?

Un switch est donc un boîtier doté de **4** à **plusieurs centaines de ports Ethernet**, et qui sert à relier en réseau différents éléments du système informatique.

Il permet

— de créer différents circuits au sein d'un même réseau,

— de recevoir des informations et d'envoyer des données vers un destinataire précis en les transportant via le **port adéquat**.

Le switch présente plusieurs avantages dans la gestion d'un parc informatique.

— Il contribue à la sécurité du réseau et à la protection des données échangées via le réseau.

— Il permet de connecter davantage de machines sur le même réseau Ethernet.

— Il permet avant tout de répartir l'information de manière "intelligente" au sein de l'entreprise.

— Il contrôle et sécurise au maximum votre réseau pour vous éviter les intrusions.

— Une fois bien paramétré, le switch distribue l'information **seulement aux utilisateurs prédéfinis en fonction de la typologie de collaborateurs** (pôle finance, direction, marketing...) et/ou de certaines restrictions, **améliorant ainsi la confidentialité des données d'entreprise.**

— Cela marche aussi dans une université par exemple ici ☺

En voici deux "beaux" spécimens

1. Celui de gauche coûte quelques euros, il est intégré dans votre box ADSL, **il est non manageable !**
2. Celui de droite coûte quelques milliers d'euros, vous l'avez vu lors du premier TP, **il est manageable !**


## 2.2 L'architecture d'un switch Ethernet

**La pièce maîtresse est le moteur de commutation.**

Il comprend une unité de contrôle de la file d'attente ainsi que des tampons entrants (***ingress***) et sortants (***egress***).

**La commutation des données s'effectue entièrement dans le matériel.**

Donc la commutation des données est possible avec un temps de **latence** très très faible, **de l'ordre de la µs.**

Oui oui, les données passent d'un port à un autre en 1µs.

**L'Adressage**

L'adressage dans un switch est basé sur les @ MAC.

Chaque machine a une adresse MAC unique au monde, exemple 01 :02 :03 :04 :05 :06.

La communication s'effectue par paquets de données (les ***frames***).

Chaque paquet de données contient

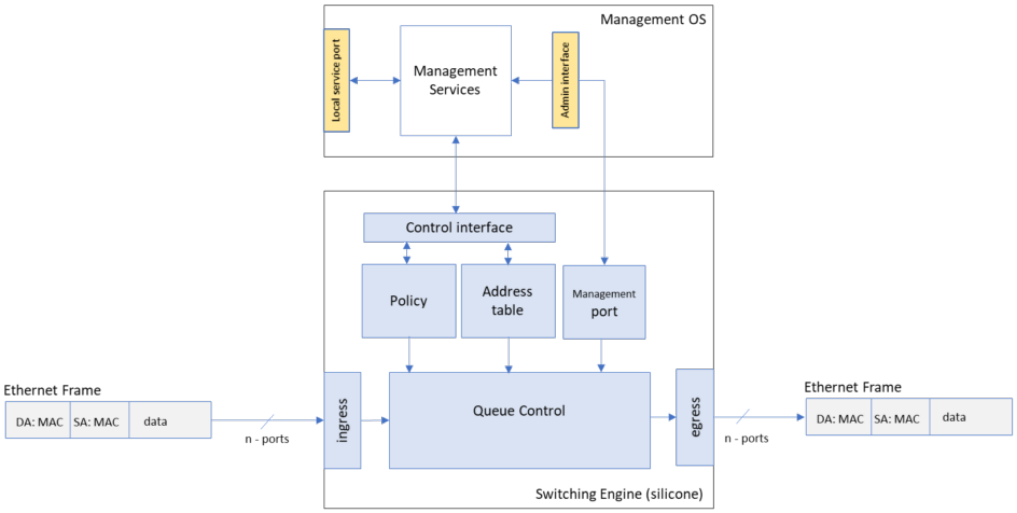
— une @ MAC de destinataire (DA)

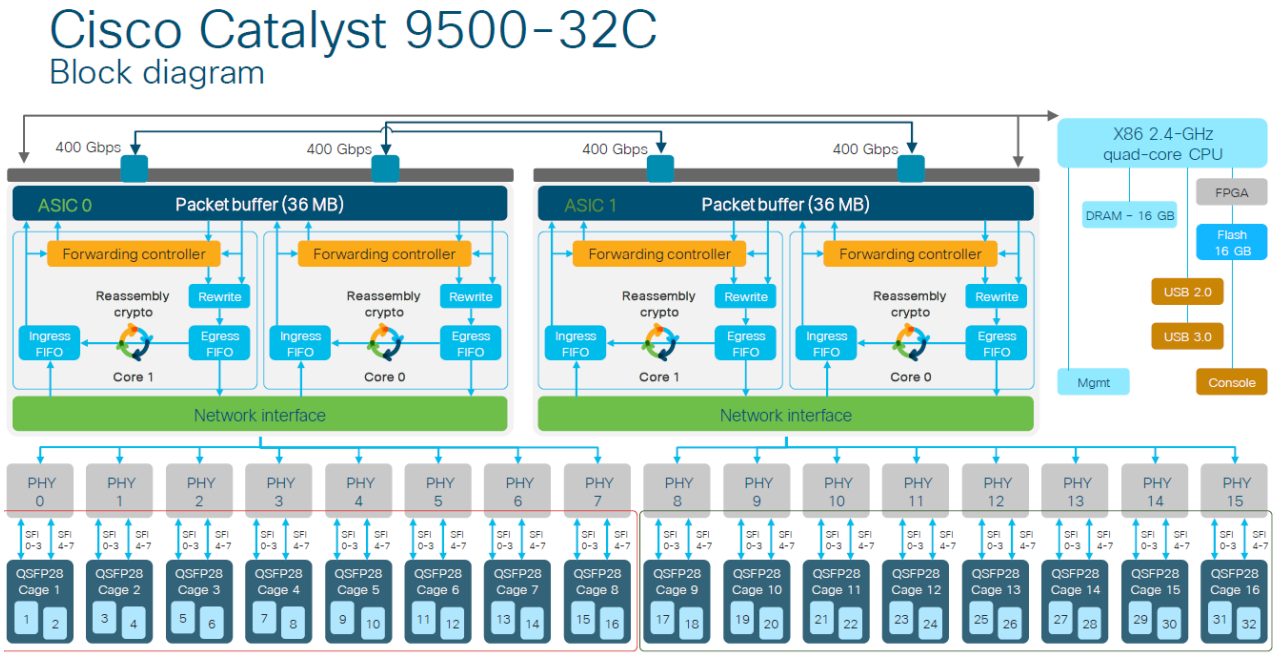
— une @ MAC d'expéditeur (SA).

**L'unité de contrôle de la file d'attente utilise l'@ DA pour décider à quel port le paquet de données entrant doit être dirigé.**

**Les @MAC sont enregistrées à cet effet dans une table MAC.**

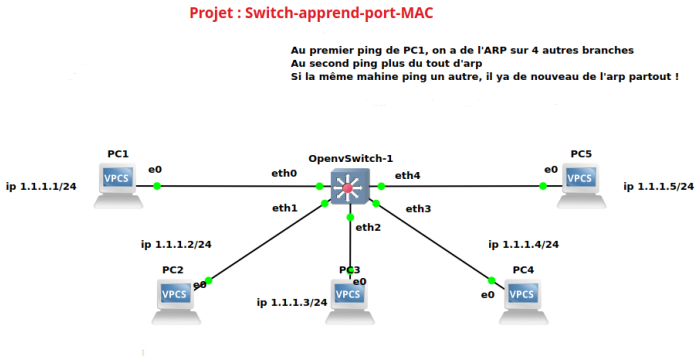
La mise à jour de la table MAC s'effectue automatiquement, l'unité de contrôle de file d'attente enregistre **l'affectation du port et de l'adresse MAC de l'expéditeur (SA)**.




Source : https://people.ucsc.edu/~warner/Bufs/9500-32C-big.PNG

L'image ci-dessous est un projet GNS3 que vous pouvez tester !




Un switch est une machine puissante d'un point de vue matériel, ce n'est pas du logiciel qui lui est lent.

Il contient autant de "µP" que l'on nomme **ASIC (*Application-Specific Integrated Circuits*)** qu'il a de ports

# 3 Les VLAN

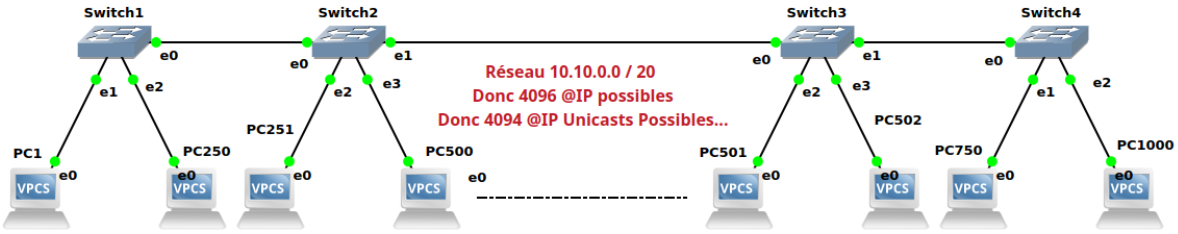
**Question** : C'est quoi un VLAN ?
**Réponse** : c'est un LAN virtuel...
La virtualisation d'un LAN consiste en la séparation entre,
— d'une part, l'infrastructure physique
— d'autre part, les services de couche 2 **liaison de données** fournis par les commutateurs.
Soit une seule infrastructure physique supporte plusieurs LAN distincts que l'on nomme VLAN

**2 machines dans le même LAN mais dans 2 VLAN différents ne communiquent pas au niveau de la couche 2**

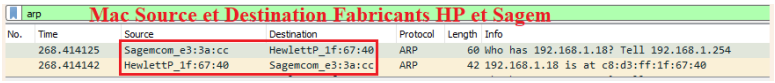
## 3.1 Pourquoi utiliser les VLAN ?

Imaginons une grande réunion de personnes (des étudiants à la FAC par exemple...) tous connectés au même switch de **plusieurs centaines de ports Ethernet**

Pour faire simple, imaginons 1000 machines connectées au même switch ou plusieurs switchs comme le montre la figure suivante et toutes sur le même réseau IP donc le **même LAN**




**Question** : Que se passe–t'il lorsque que l'un deux veux contacter un autre ?
Réponse : Il y a une tempête de **999 requêtes ARP** qui traversent les switchs !
Si si souvenez vous : Qui à cette @IP demande 192.168.1.254...
et un seul va répondre si il répond ☺




Et pendant ce temps personne ne peut travailler ! ! !
Donc on va découper ce LAN en plusieurs VLAN.

**Autre possibilité** : Imaginons un immeuble, très grand immeuble tels ceux de la défense à Paris ou bien à Manhattan, ou pourquoi pas le CHU de Caen
Nous sommes dans la même situation, tous les ports Ethernet sont câblés, les câbles descendent dans des goulottes et au sous-sol il y a plein plein de switchs pour tous les relier au niveau de la couche 2 du modèle OSI.
Vous imaginez un employé de l'entreprise X **root** sur sa machine qui lance wireshark et qui écoute tout ce qui se passe ... ce ne serait pas très "***secure***"
**Ce serait bien de pouvoir séparer les ports non ?**
**Oui ?**
**Alors on fait des VLAN.**

## 3.2 Les 3 types de VLAN

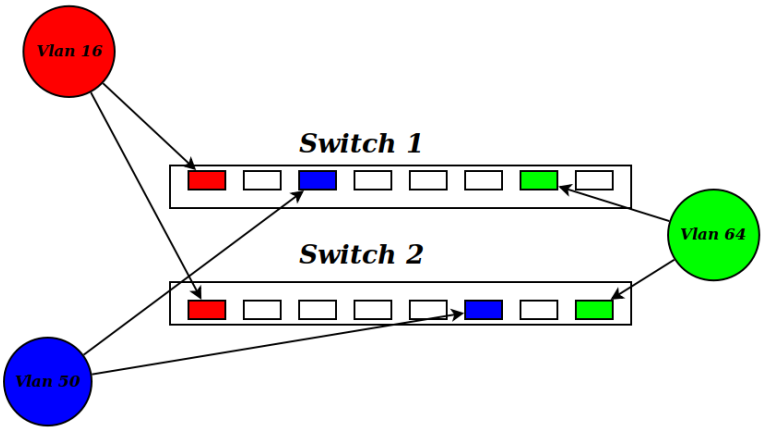
Les différents types d'association aux VLANs
Dans les matériels réseaux, l'association d'un VLAN à un port se fait par un table d'association. ...

1. VLAN de niveau 1 aussi appelé **VLAN par port** : C'est le mode d'association par défaut. ...
2. VLAN de niveau 2 aussi appelé **VLAN par adresse MAC**
3. VLAN de niveau 3 aussi appelé **VLAN par adresse IP**

Ça veut dire quoi ces 3 types de VLAN ?

### 3.2.1 Niveau 1 : Les VLAN par port

**Les Vlans par port associent un port d'un switch à un numéro de Vlan.**
On dit alors que le port est tagué suivant le Vlan donné.
Le switch entretien ensuite une table qui lie chaque Vlan au port associé.
Le taggage des ports peut se faire de manière statique ou de manière dynamique. Voir la norme 802.1q




— Les **avantages** :
l'avantage principale du Vlan par port est qu'il permet une **étanchéité maximale** des Vlans.
Une attaque extérieur ne peut être possible se faire qu'en **branchant le PC pirate sur un port tagué**.
Le pirate a donc besoin d'avoir **accès à la machine physique** pour pénétrer le Vlan.
Le Vlan par port offre une facilité de configuration.
L'administrateur réseau peut sans grande difficulté choisir les ports à taguer sans avoir quelconque information des machines auxquelles sont reliés les ports.

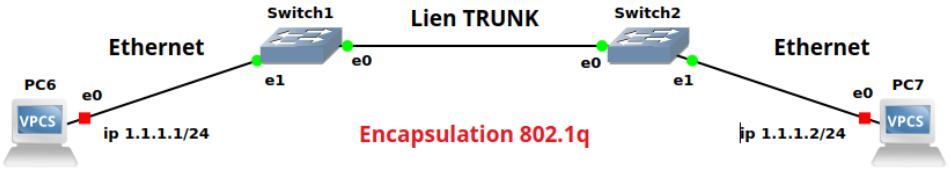
— Les **inconvénients** :
L'inconvénient principal de la technologie du Vlan par port est qu'il nécessite une configuration lourde et contraignante **sur chaque switch**.
À chaque déplacement d'une machine, il faut modifier la configuration des switchs correspondant.
Le mécanisme de Vlan par port ne possède pas d'architecture centralisée qui pourrait permettre d'éviter la lourdeur de la configuration.
Chaque switch possède sa table de correspondance (VLAN <–> port) indépendamment du contenu des autres switchs.

### 3.2.2 Niveau 2 : Les VLAN par adresse MAC

**Le Vlan par adresse MAC segmente le réseau en fonction de l'adresse MAC de l'utilisateur.**
On associe ainsi des adresses à des Vlans pour permettre à un utilisateur de se déplacer sans changer de profil.
**Ce type de Vlan est utilisé pour regrouper les utilisateurs par service.**
Ce type de Vlan permet de **regrouper** au sein d'un même lien et de les transporter sur le réseau.

— Les **avantages** :
Les Vlans de niveau 2 permettent une sécurité au niveau de l'adresse MAC, c'est à dire qu'un pirate voulant se connecter sur le Vlan devra avant récupérer une adresse MAC du Vlan pour pouvoir entrer.
Les Vlans de niveau 2 offrent des possibilités de centralisation des tables Vlans adresses MAC.
Chaque Switch interroge ensuite cette table pour connaître les informations nécessaires à une adresse MAC donnée.

— Les **inconvénients** :
Le Vlan de niveau 2 offre une sécurité moindre que le Vlan par port de par la possibilité de modifier l'adresse MAC.




### 3.2.3 Niveau 3 : VLAN par adresse IP ou sous réseau

**Principe** :

Les Vlans de niveau 3 permettent de regrouper plusieurs machines suivant le sous réseau auquel elles appartiennent.

La mise en place de Vlan de niveau 3 est conditionné par l'utilisation d'un protocole dit routable donc la couche 3 la couche IP.

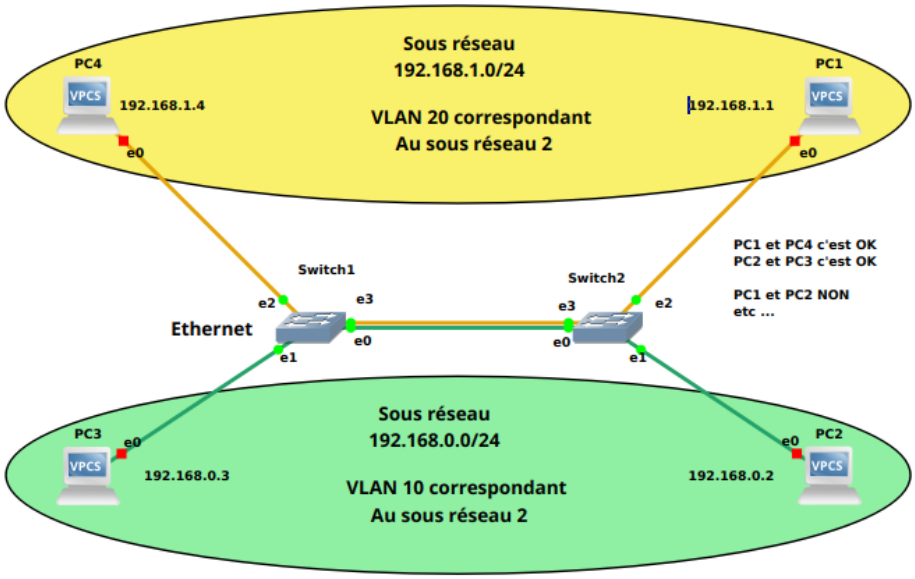
L'attribution des Vlans se fait de manière automatique en décapsulant le paquet jusqu'à l'adresse source.

Cette adresse détermine à quel Vlan appartient la machine.

La fac utilise cela !

— Les **avantages** : L'avantage du Vlan de niveau 3 est qu'il permet une **affectation automatique à un Vlan suivant une adresse IP**.
Par conséquent, il suffit de configurer les clients pour joindre les groupes souhaités.
Il est aussi possible de séparer les protocoles par Vlan.

— Les **inconvénients** : Les Vlans de niveau 3 sont lents par rapport aux Vlans de niveau 1 et 2.
Le switch est obligé de dés encapsuler le paquet jusqu'à l'adresse IP pour pouvoir détecter à quel Vlan il appartient.
Il faut donc des équipements plus onéreux, des switchs de niveaux 3 (car ils doivent pouvoir décapsuler le niveau 3) pour une performance moindre.
La sécurité est beaucoup plus faible par rapport aux Vlans de niveau 1 et 2.
L'analyse de l'adresse IP rend le *spoofing*[1] IP possible.
Et le *spoofing* IP est beaucoup plus simple à réaliser que le *spoofing* MAC.
Les Vlans de niveau 3 sont restreints par l'utilisation d'un protocole de routage pour avoir l'identifiant niveau 3, et ainsi se joindre au Vlan correspondant.



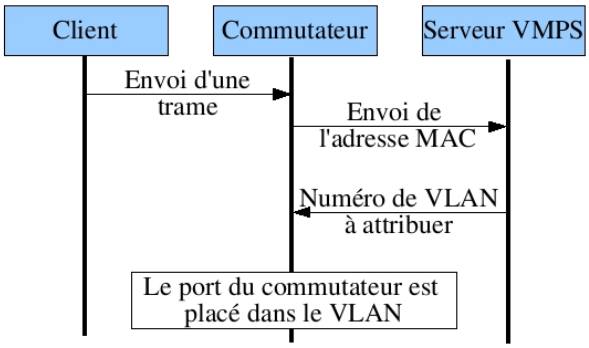

Nous le ferons en TP ☺

1. *usurpation d'identité*

### 3.2.4 Pour aller plus loin dans la sécurité

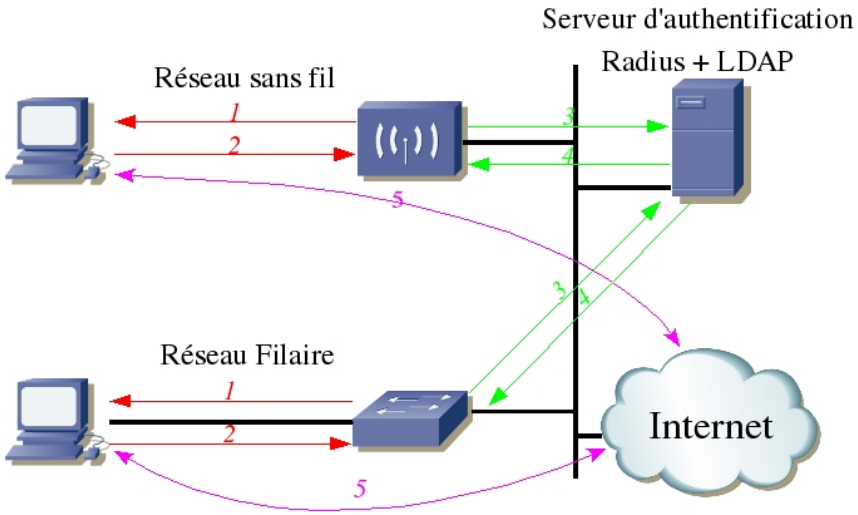
Cette partie ne sera pas évaluée au CT, juste pour information pour ceux qui voudraient poursuivre dans ce domaine...

**3.2.4.1 Le VMPS** La gestion de Vlans est fastidieuse et rébarbative sur les grands sites hétérogènes !
Il faut trouver une solution pour **automatiser** cette gestion.
VPMS (***Vlan Membership Policy Server***) est un service, créé par Cisco et que sur les commutateurs Cisco..., chargé de faire correspondre un Vlan à une ou plusieurs @MAC et s'impose donc comme la solution.
Le principe :




**Le protocole VMPS n'est pas une solution d'authentification, c'est une solution d'identification.**
On ne garantit pas l'utilisateur présent face à la machine, on enregistre juste quelle machine s'est connectée.
**C'est donc une mesure temporaire qui est remplacée par 802.1x !**

**3.2.4.2 Le 802.1x** La norme 802.1x est un standard IEEE qui a pour objectif la **vérification de l'authentification avant la connexion de l'ordinateur au réseau**.
Une fois cette authentification effectuée, **l'ordinateur est placé dans le VLAN déterminé** par le serveur d'authentification centralisé (**RADIUS**).
Par défaut, un port de commutateur est fermé.
Dès qu'un ordinateur se connecte, le commutateur active le port en ne laissant passer que les trames 802.1x.
Cela marche en Wifi et en filaire
L'image suivante explique le principe.



1. Le switch demande alors à l'ordinateur de s'authentifier ou d'authentifier l'utilisateur qui est face à cet ordinateur.

   Si l'ordinateur "comprend" la demande. Il faut pour cela un logiciel d'authentification activé
2. Le switch met en relation le serveur RADIUS (***Remote Authentication Dial-In User Service***) central et l'ordinateur client
3. Le client envoie l'information d'authentification au serveur RADIUS.

   Celui-ci s'adresse à l'annuaire LDAP (***Lightweight Directory Access Protocol***) pour vérification.
4. Si l'annuaire LDAP confirme l'authentification, le serveur RADIUS **demande au switch de mettre le port dans un VLAN particulier** et d'**activer le port**.
5. L'ordinateur a accès au réseau.

   Il peut alors demander une @IP par DHCP, une passerelle et une @IP de DNS.

   Il n'y a plus de cryptage entre l'ordinateur et le réseau.

**Authentification**

Par mesure de sécurité, **toutes les communications de l'authentification sont chiffrées**.

Il existe plusieurs types de chiffrement disponibles pour la communication entre un serveur RADIUS et le client.

Parmi eux le **EAP-TTLS** (***Extended Authentication Protocol - Tunneled Transport Layer Security***), qui demande par contre l'installation d'un logiciel sur les postes clients.

Le principe de TTLS est le suivant :

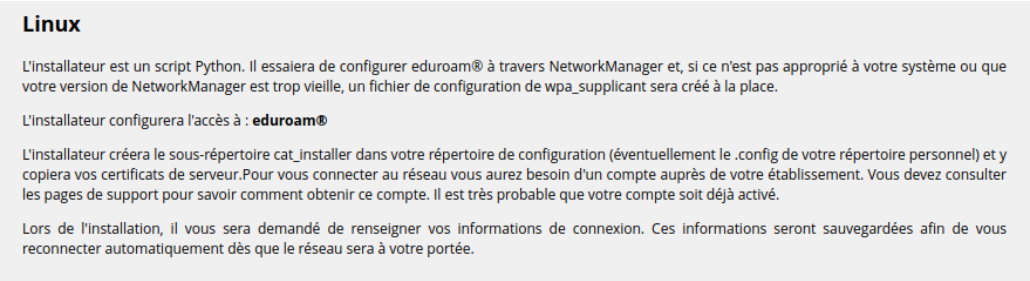
— Le serveur RADIUS envoie au client un certificat électronique **CA** ;
— Le client vérifie ce certificat. Le client doit avoir les **CA** de certification ;
— Le client demande le **login** et le **MDP** de l'utilisateur ;
— Un **tunnel chiffré** est généré entre le client et le serveur RADIUS ;
— Le **MDP** est envoyé dans le tunnel TLS ;
— Le serveur RADIUS reçoit le mot de passe et le fait vérifier par l'annuaire LDAP. L'annuaire LDAP vérifie aussi si l'utilisateur est autorisé dans le réseau qu'il demande ;
— Le serveur RADIUS autorise ou pas la connexion auprès du commutateur.

## La fac de Caen utilise le 802.1x

https://catalogue-de-services.unicaen.fr/service/gestion-fiche/afficher/440?lang=fr

Vus pouvez aller sur le site : https://www.eduroam.fr/

Si vous voulez sous Linux, il y a un script python ☺



**Linux**

L'installateur est un script Python. Il essaiera de configurer eduroam® à travers NetworkManager et, si ce n'est pas approprié à votre système ou que votre version de NetworkManager est trop vieille, un fichier de configuration de wpa_supplicant sera créé à la place.

L'installateur configurera l'accès à : **eduroam®**

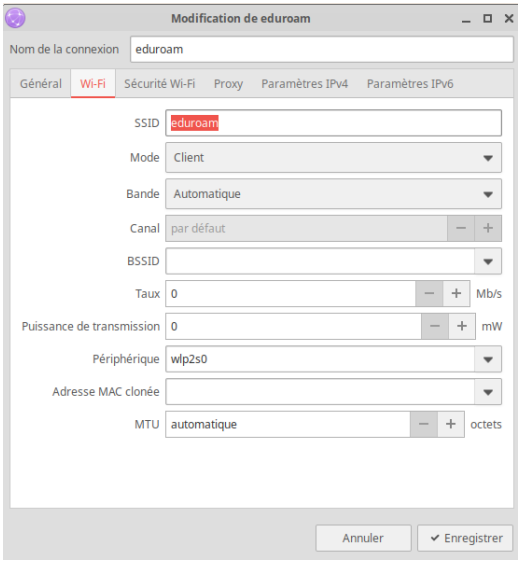
L'installateur créera le sous-répertoire cat_installer dans votre répertoire de configuration (éventuellement le .config de votre répertoire personnel) et y copiera vos certificats de serveur.Pour vous connecter au réseau vous aurez besoin d'un compte auprès de votre établissement. Vous devez consulter les pages de support pour savoir comment obtenir ce compte. Il est très probable que votre compte soit déjà activé.

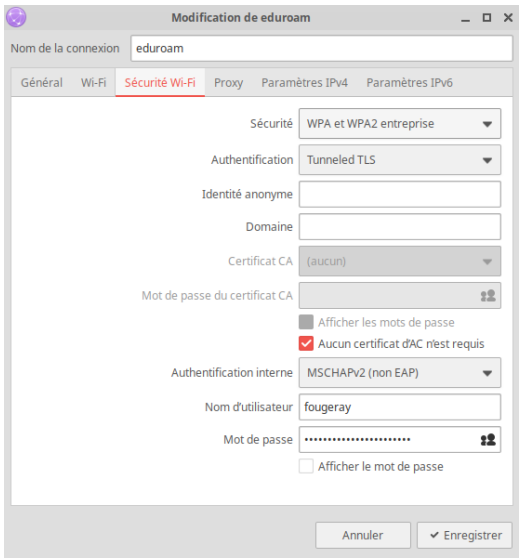
Lors de l'installation, il vous sera demandé de renseigner vos informations de connexion. Ces informations seront sauvegardées afin de vous reconnecter automatiquement dès que le réseau sera à votre portée.

Accès au service

1. **Sélectionner** le réseau eduroam dans la liste des réseaux proposés ou SSID réseau : eduroam
2. anonymous-identity=anonymous@unicaen.fr
3. Sécurité : « 802.1x Entreprise »
4. **Choisir** "TTLS" pour la méthode d'authentification EAP
5. **Choisir** "MSCHAPv2" pour l'authentification phase 2
6. "Ne pas valider" pour le certificat CA
7. Renseigner votre identifiant de connexion et votre mot de passe : identifiant@unicaen.fr
8. Cliquer sur "se connecter"

Et ça donne cela ...



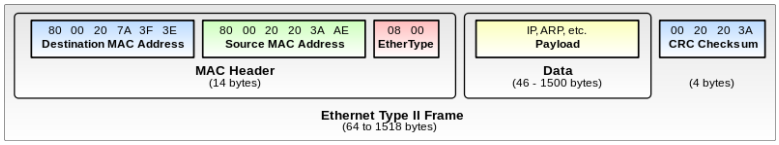




## 3.3 Comment sait-on que c'est un VLAN et non un LAN ?

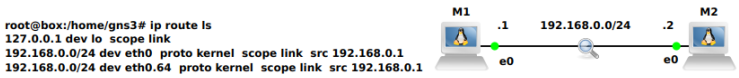
Quand une trame Ethernet arrive, comment sait-on que c'est un VLAN et non un LAN ?
**Réponse** : La machine regarde l'**ethertype**
Mais si rappelez vous le cours sur Ethernet, le premier CM ☺

— **EtherType** : codé sur 2 octets, indique le type de protocole inséré dans le champ donnée.
Quelques valeurs

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **0x0800** | **0x0806** | 0x86DD | **0x8100** | **0x8847** | 0x8870 | | | | 0xCAFE |
| **IPv4** | **ARP** | IPv6 | **VLAN** | **MPLS Unicast** | Jumbo Frames | | | | oui oui ^^ |




Soit la structure suivante :




Les 2 machines M1 et M2 sont reliées par **un même et seul câble !**
Sur M1 on lance les commandes suivantes

```
ifconfig eth0 192.168.0.1 netmask 255.255.255.0
ip link add link eth1 name eth1.64 type vlan id 64
ifconfig eth1.64 192.168.0.1 netmask 255.255.255.0
```

```
root@box:/home/M1# ip route ls
127.0.0.1 dev lo scope link
192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.1
192.168.0.0/24 dev eth0.64 proto kernel scope link src 192.168.0.1
```

Sur M2 on lance les commandes suivantes

```
ifconfig eth0 192.168.0.2 netmask 255.255.255.0
ip link add link eth1 name eth1.64 type vlan id 64
ifconfig eth1.64 192.168.0.2 netmask 255.255.255.0
```

```
root@box:/home/M1# ip route ls
127.0.0.1 dev lo scope link
192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.2
192.168.0.0/24 dev eth0.64 proto kernel scope link src 192.168.0.2
```

On voit que M1 et M2 ont deux interfaces nommées **eth0** et **eth0.64**

**eth0.64** est une sous interface, mais une interface quand même qui fonctionne comme une interface, la preuve

Un ping de M1 vers M2 peut se faire de 2 manières

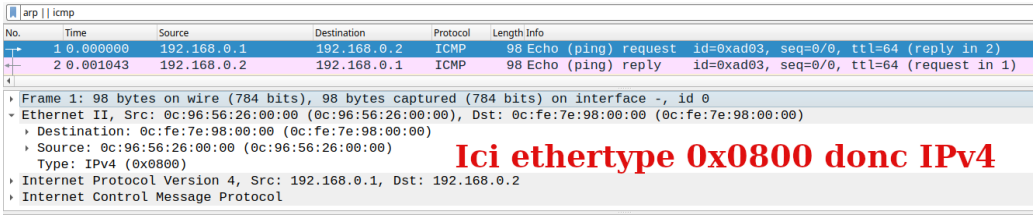
1. ***ping 192.168.0.2***

   ou

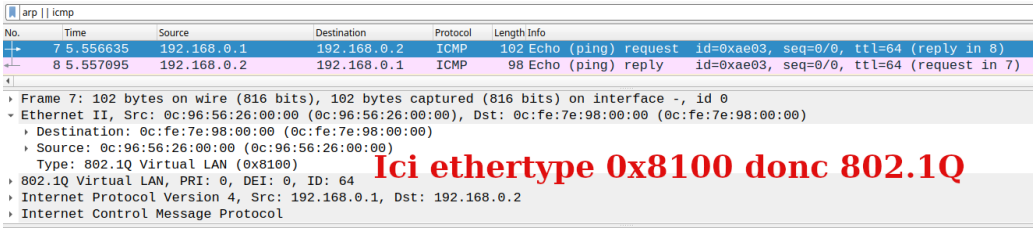
2. ***ping 192.168.0.2 -I eth0.64***

l'option **-I** de **ping** indique quelle interface utiliser

Ici l'**ethertype** est 0800 donc on sait que la suite c'est de l'IP !




Si l'**ethertype** est 0x8100 c'est un Virtual LAN




### 3.3.1 une trame Ethernet avant et après le vlan

La norme IEEE 802.1q : Standardisée et interopérable, ajoute une étiquette dans l'en-tête de la trame, un ensemble de champs juste après le champ d'adresse MAC d'origine.

Cette étiquette a une taille de 32 bits dont **12 bits sont consacrés au numéro de VLAN.**

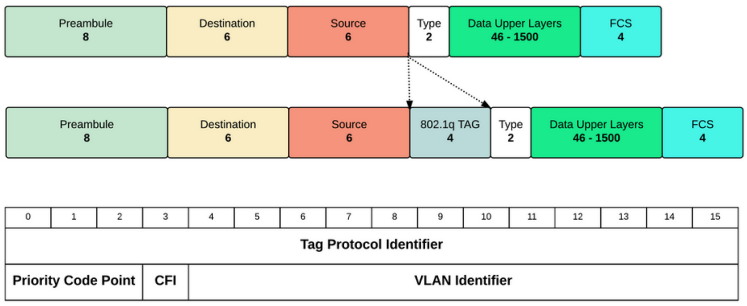
Le standard supporte les technologies :

— IEEE 802.3 (Ethernet),

— IEEE 802.11 (WIFI),

— Et d'autres sans intérêt !

**Vu que la trame sera modifiée, le commutateur recalculera la valeur du champ CRC/FCS.**




### 3.3.2 Combien de VLANs ?

La tag du VLAN étant codé sur 12 bits on a **4096** vlans différents

Pas dans le monde !

Non dans une entreprise !

Ce qui laisse de la marge ☺

### 3.4 Trunk ou comment mettre plusieurs vlans dans un seul fil ?

C'est quoi un **trunk** et bien c'est le tronc de l'arbre où toutes les branches de l'arbre se rejoignent.
Mais dans le domaine des réseaux ?
Voyons la situation suivante.
Plusieurs vlans doivent rejoindre la même passerelle ou bien plusieurs vlans sur un switchs doivent rejoindre plusieurs vlan de même identifiant
On parle de **trunk** ou de **liaison d'agrégation**
Le port du switch autorisera plusieurs vlans à passer par lui.
Je ne vais pas m'attarder sur cette notion que l'on verra en TP ☺

## 4 Le routage inter vlan

**Rappels** :
— Un switch ou pont ou bridge ne sait travailler que sur la couche 2 du modèle OSI
— Deux machines dans 2 vlans différents ne peuvent communiquer !
— S'il faut changer de réseau on est obligé de passer par une machine spéciale que l'on nomme **un routeur** et qui elle travaille sur la couche 3 du modèle OSI !

La solution logique est donc de mettre un routeur et se débrouiller pour qu'il fasse le lien au niveau de la couche 3

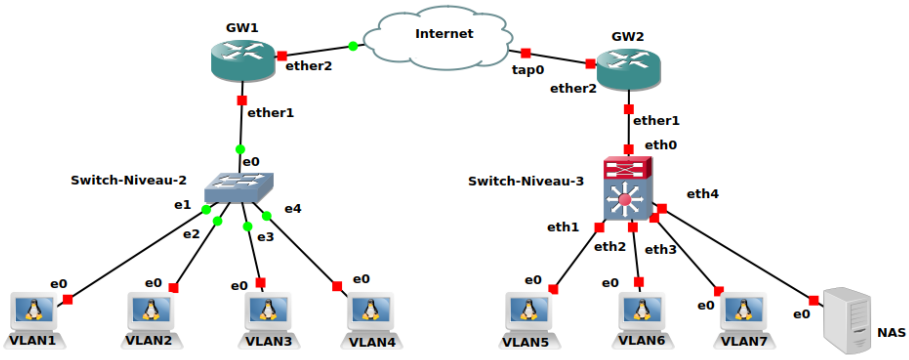
### 4.1 Comment ça se passe si on fait le routage inter-vlan au niveau du routeur ?

**Et bien ça marche parfaitement jusqu'à ce que l'on rencontre un cas particulier !**
**C'est viable si les quantités de données échangées ne sont pas trop importantes !**

Imaginons la situation suivante.
— Un **NAS** (***Network Attached Storage*** ou serveur de stockage en réseau) situé dans **un VLAN**
— Des machines se connectant à ce NAS dans un **autre VLAN**.
— Si on fait le routage du trafic inter vlan au niveau du routeur, les performances possibles entre machines et le NAS, serveur de fichiers risques d'être moindre.
C'est d'autant plus vrai si vous reliez ce serveur en plusieurs fois 1 Gbps ou en 10 Gbps et que vous avez mettons un routeur connecté en 1 Gbps sur le réseau : il sera limité à la fois par
  — son interface Ethernet,
  — son CPU
  — sa mémoire de travail (RAM)

En utilisant, dans un réseau très très sollicité, le routeur, qui fait aussi office de passerelle Internet pour le routage inter-VLAN, on risque de dégrader les performances du réseau.

La **solution** : Utiliser **un switch de niveau 3**
C'est quoi cette bête ?
C'est un alien ? ☺
Non, c'est un switch auquel on a incorporé quelques fonctions de routage. Il sait travailler sur la couche 2 et la couche 3.
Il peut remplacer dans certaines situations un routeur.
C'est avant tout un switch ! ! !
Quand on passe sur des switchs de niveau 3, on peut déplacer le point où se fait le routage entre les vlans sur le ou les switchs et bénéficier ainsi de leur capacité de routage **sans commune mesure avec celle des vrais routeurs.**
Cela est lié au fait que les switchs utilisent des puces spécifiques les **ASIC** (***Application-Specific Integrated Circuits***) pour le niveau 3 ce qui n'est jamais le cas des routeurs installés en entreprise et qui servent de GW.
L'image ci-dessous illustre les 2 cas
— À gauche c'est GW1 qui fait le routage inter vlan
— À droite c'est le switch de niveau 3 qui fait le routage inter vlan




En TP nous ne ferrons pas cela, pour différentes raisons
— Pas le matériel
— Pas le temps

## 4.2 Comparaison Switch de niveau 2 et 3

| Éléments | Switch de niveau 2 | Switch de niveau 3 |
|---|---|---|
| Fonction de routage | Uniquement @ MAC | Prise en charge d'un routage supérieur tel que le routage statique et dynamique |
| Balisage vlan en fonction de l'@ IP | Non | Oui |
| Inter vlan | Non | Oui |
| Scénario d'utilisation | Domaine de couche 2 pure | Agrégation de switchs d'accès multiples |

En TP nous ne verrons que les switchs de niveau 2 ☹

## 4.3 Comparaison Switch de niveau 3 et routeur

Les caractéristiques fondamentales du switch de niveau 3 et du routeur

| Caractéristiques | Switch niveau 3 | Routeur |
|---|---|---|
| **Routage de base couche 3** | Oui | Oui |
| Gestion du trafic | Oui | Oui |
| Support pour carte WIC | Non | Oui |
| Fonctions de routage avancées | Non | Oui |
| **Architecture de transmission** | **Matériel-ASIC** | **Logiciel** |
| Support RMON | Oui | Non |
| Qualité de politique | Élevée | Basse |
| Support WAN | Non | Oui |
| Interfaces WAN | Non | Oui |
| Caractéristiques QoS | Non | Oui |
| **NAT** (Traduction d'adresse réseau) | Non | Oui |
| Fonctionnalités **LAN** | Oui | Non |

**À retenir** :
— Un switch de niveau 3 ça existe, c'est un "switch" que l'on met quand on a besoin de beaucoup de bande passante entre plusieurs vlans
— Un switch de niveau 3 ne remplace pas un routeur !
— Un switch de niveau 2 fait du routage @ MAC
— Un routeur fait du routage @ IP
— Votre box chez vous c'est
  — un routeur qui fait du NAT
  — un switch
  — une AP (***WiFi Access Points***)

— un serveur DHCP
— un serveur DNS
— etc ...

# 5 Sous Linux

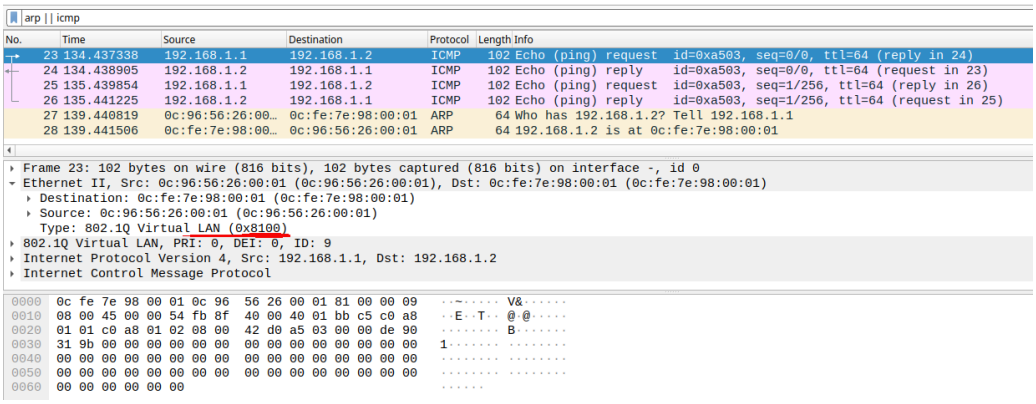
Il est facile de créer des Vlans sous Linux.
Il suffit de créer des **sous interfaces**.
Nous allons le faire en TP.
Voir le projet : **vlan-avec-Microrelinux.**
Voyons la structure suivante
Nous avons 2 machines ayant chacune **qu'une seule interface** !


**Attention la commande ifconfig ne permet pas de voir les sous interfaces !**
On passe root sur les 2 PC : ***sudo su***

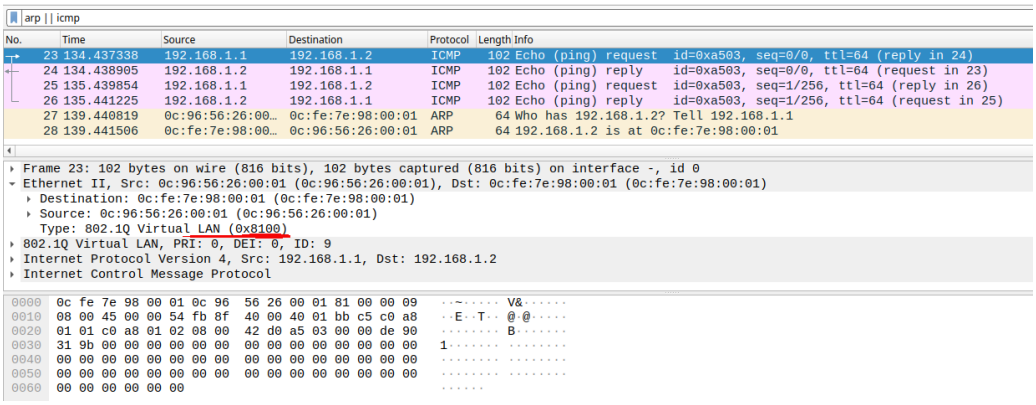
Sur M1 on lance :

— ***ifconfig eth0 192.168.0.1 netmask 255.255.255.0***
— ***ip link add link eth0 name eth0.64 type vlan id 64***
— **ip a show eth0.64** renvoie l'@ MAC de la sous interface eth0.64

Sur M2 on lance les mêmes commandes en ne changeant que l'IP qui passe de .1 à .2 !
Puis voyons si M1 peut pinguer M2 via cette sous interface, la réponse devrait être positive donc oui.
Comme le montre la capture wireshark suivante :
On peut voir le **Tag 9** entre les **couches 2 et 3.**




Si on développe la couche 2 on peut voir que le type **Ethertype** n'est pas IP **(0x0800)** au dessus mais **802.1Q Virtual LAN (0x8100)**




Si nous faisons la même manipulation en créant 2 sous interfaces sans le même Tag elles ne pourront pas se "pinguer"

Sur M1 on lance :

— ***ip link add link eth1 name eth1.64 type vlan id 64***
— Un ***ip a show eth1.9*** renvoie l'@ MAC de la sous interface eth1.9
— ***ifconfig eth1.64 192.168.2.1*** (Par défaut on aura un /24)

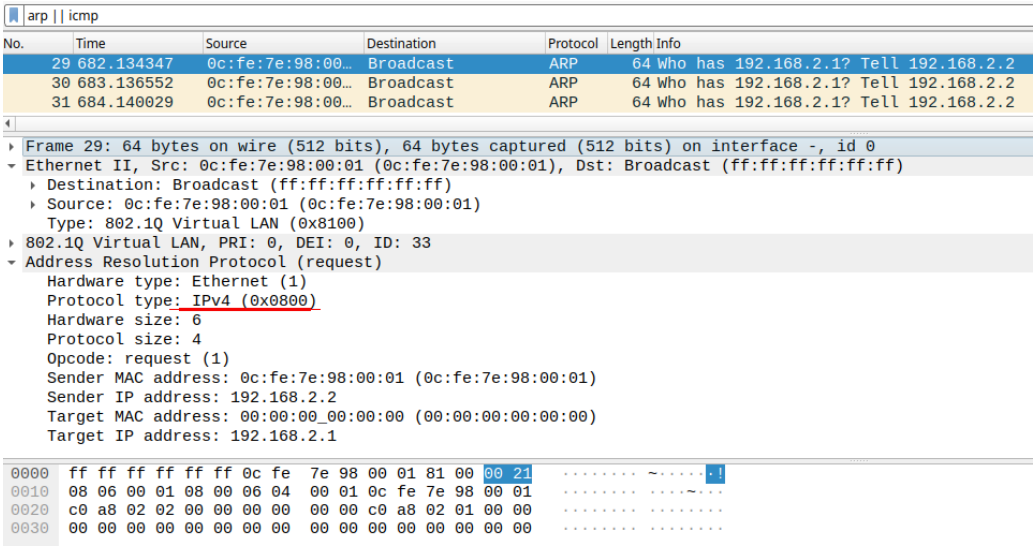
Sur M2 on lance :

— ***ip link add link eth1 name eth1.33 type vlan id 33***
— ***ifconfig eth1.33 192.168.2.1***

Un ping de M2 vers M1 ou de M1 vers M2 en passant par le réseau 192.168.2.0/20 ne marche pas ! ! ! car pas le même Tag ! ! !

Une capture wireshark montre la requête ARP à destination de Broadcast (MAC ff :ff :ff :ff :ff :ff) qui n'aboutit pas !

Donc le Ping ne pourra pas fonctionner ! ! !




Si on lance la commande ***ip a*** et ***arp -a*** sur les 2 PC on obtient quelque chose comme :

Pour M1

```
root@box:/home/gns3# ip a
6: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 0c:96:56:26:00:01 brd ff:ff:ff:ff:ff:ff
7: eth1.9@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 0c:96:56:26:00:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global eth1.9
       valid_lft forever preferred_lft forever
8: eth1.64@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 0c:96:56:26:00:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/24 brd 192.168.2.255 scope global eth1.64
       valid_lft forever preferred_lft forever
root@box:/home/gns3# arp -a
? (192.168.1.2) at 0c:fe:7e:98:00:01 [ether]  on eth1.9
```

Pour M2

```
root@box:/home/gns3# ip a
6: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 0c:fe:7e:98:00:01 brd ff:ff:ff:ff:ff:ff
7: eth1.9@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 0c:fe:7e:98:00:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.2/24 brd 192.168.1.255 scope global eth1.9
       valid_lft forever preferred_lft forever
8: eth1.33@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 0c:fe:7e:98:00:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.2/24 brd 192.168.2.255 scope global eth1.33
       valid_lft forever preferred_lft forever
root@box:/home/gns3# arp -a
```

```
? (192.168.2.1) at <incomplete>  on eth1.33
? (192.168.1.1) at 0c:96:56:26:00:01 [ether]  on eth1.9
root@box:/home/gns3#
```

On vient de fabriquer des switchs avec des VLANs

Oui, oui, les switchs sont actuellement des machines sous linux
Si on lance les commandes ***modinfo 802.1q*** et ***lsmod*** sous ces 2 PC on obtient :

```
root@box:/home/gns3# modinfo 8021q
filename:       kernel/net/8021q/8021q.ko.gz
license:        GPL
version:        1.8
alias:          rtnl-link-vlan
srcversion:     594EBB6763374BE3D856132
depends:        mrp,garp
vermagic:       3.16.6-tinycore SMP mod_unload 486
root@box:/home/gns3# lsmod
Module                  Size  Used by    Not tainted
8021q                  20480  0
mrp                    12288  1 8021q
garp                   12288  1 8021q
stp                    12288  1 garp
llc                    12288  2 garp,stp
...
root@box:/home/gns3#
```

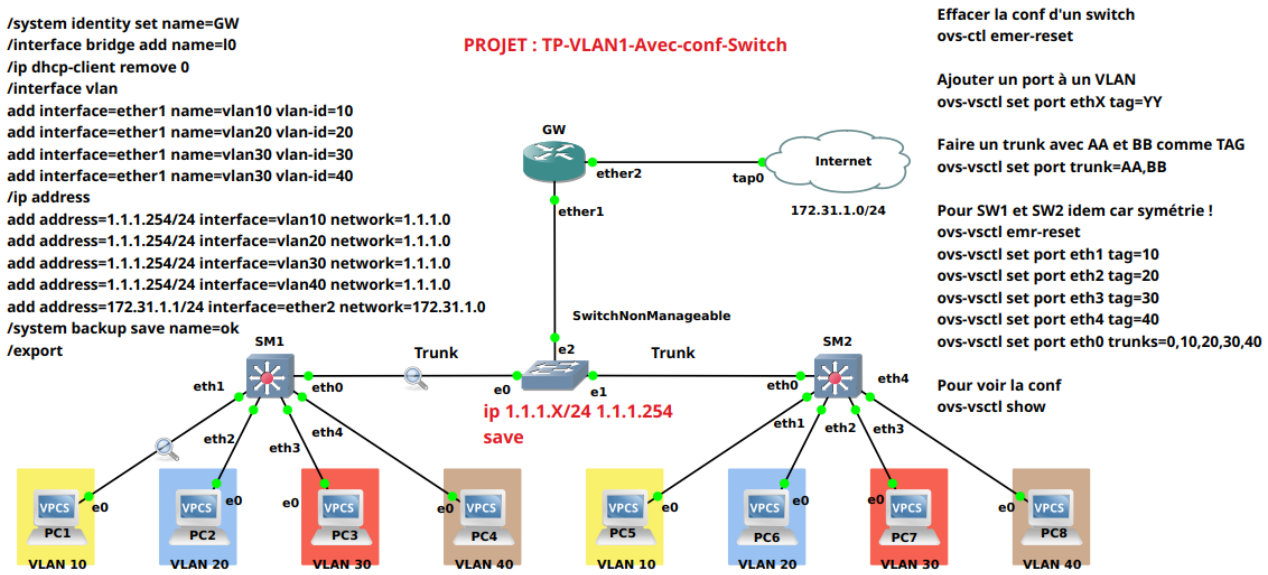
Vous pourrez si vous avez le temps et l'envie lancer ces commandes dans la VM où vous êtes root ou bien sur votre linux personnel.
Pas les PC de la FAC, vous ne pouvez pas être root ! ! !

# 6 Configuration plus avancée

Dans cette partie nous allons voir une maquette un peu plus "professionnelle".
Pour cela nous allons utiliser les switchs en libre utilisation :
OpenvSwitch https://www.openvswitch.org/
Des switchs virtuels qui n'ont pas autant de fonctions que les switchs réels "professionnels" mais seront suffisants pour nous ☺
Il est en effet impossible d'utiliser même en virtualisation les switchs de chez Cisco qui sont payants et très très très chers ... ☹
Sur ce site une minidoc
https://mesangebleue.github.io/OpenVSwitch_CheatSheet/

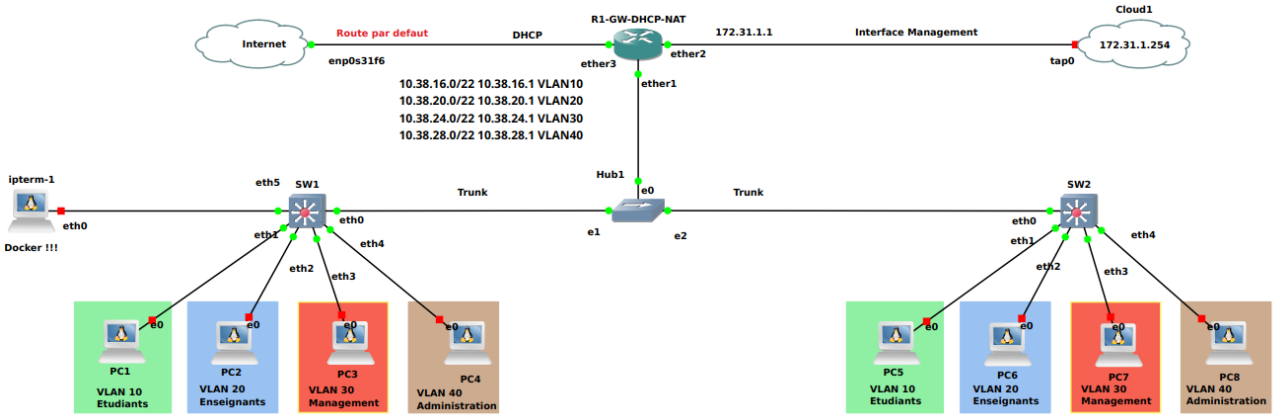
## 6.1 Exemple simple TP VLAN-1

C'est le projet **TP-VLAN1-Sans-conf-Switch**




## 6.2 Exemple plus complexe TP VLAN-2

C'est le projet **TP-VLAN2-DHCP-GW-Firewall**




# 7 Conclusion

Oui ce cours fut long, mais nous avons fini de traiter la couche 2 ☺

Maintenant vous savez ce qu'est un pont, un bridge un switch, une interface, une sous-interface, un port, un tag, un trunk, un Lan, un vlan, un switch de niveau 3, le routage inter-vlan etc ...

Il n'existe aucune organisation, société, entreprise qui n'utilise pas ces technologies.