Module M2102
Architecture des réseaux

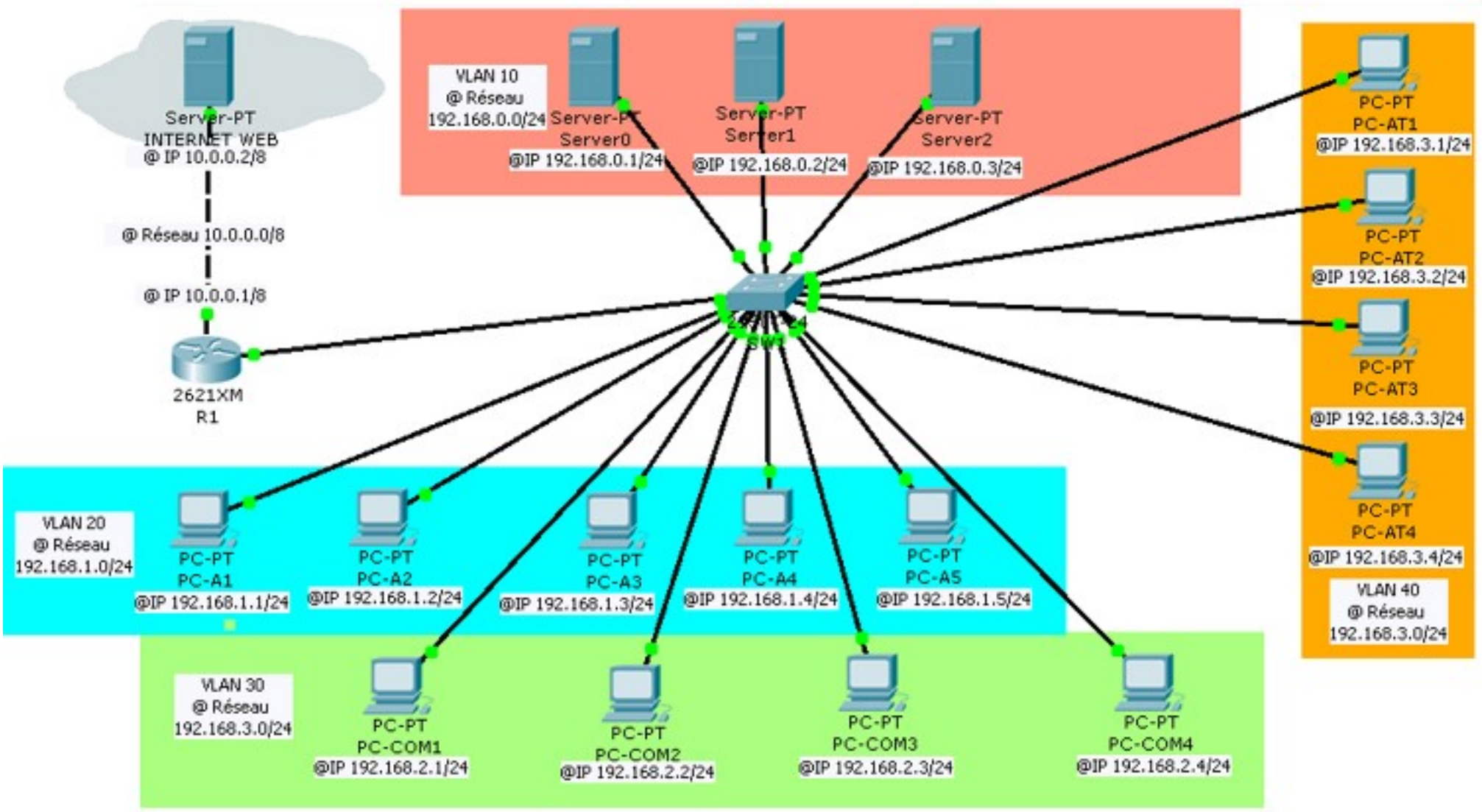
Chapitre 4

Réseaux locaux virtuels
VLAN

Lectures préalables :

- VLAN sur wikipedia
- VLAN sur wikibooks

Exemple : 4 VLANs et un switch2-3

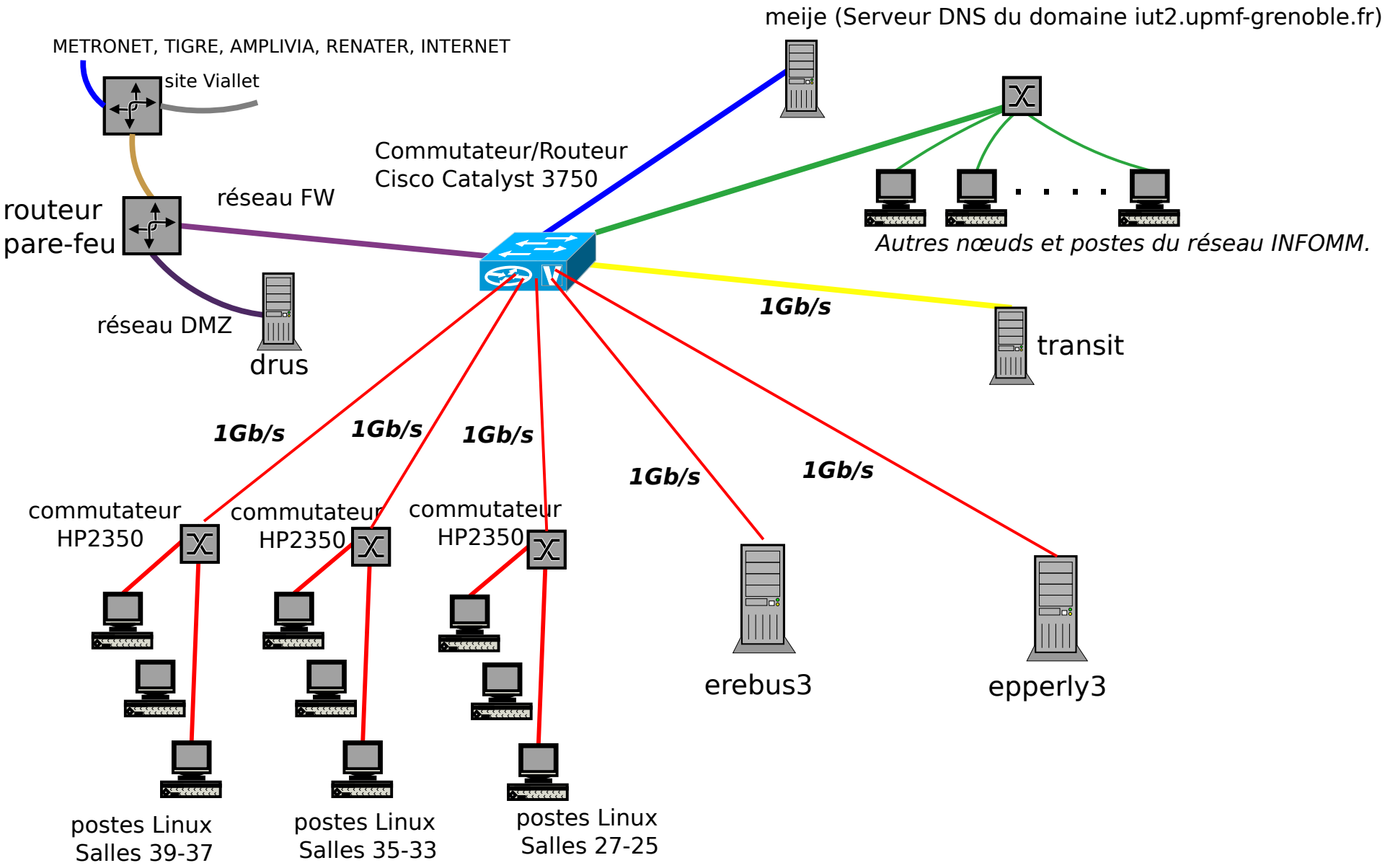


Source : **http://www.tech.agopyan.fr/Cisco/Images/im-pac-tr.png**

Vocabulaire

- **Réseau local virtuel** (VLAN : Virtual Local Area Network) :
  - Réseau local : technologie Ethernet (ou Wi-Fi).
  - Virtuel : dissociation entre la structure matérielle du réseau et la définition de réseaux IP.
  - Principe : diviser un réseau local (physique) en plusieurs réseaux logiques (IP) appelés VLAN.
  - Équipement qui permet cette organisation en VLAN : le switch2-3 ou commutateur-routeur.
- **Switch2-3** (ou commutateur-routeur, ou switch multi-niveaux). Il assure à la fois :
  - Une fonction de commutation Ethernet (niveau liaison ou niveau « MAC » des réseaux locaux = niveau 2).
  - Une fonction de routage IP (niveau réseau = niveau 3).

Le switch2-3 de l'IUT2



Description du Cisco Catalyst 3750

- 24 (48) ports Ethernet 100Mb/s, 2 (4) ports Gigabit Ethernet.
- Facilité d'utilisation, de déploiement et d'évolution (interface web, auto-configuration, auto-négociation, empilement).
- Redondance pour assurer le service en cas de défaillance.
- Qualité de service : gestion de trafic différenciée selon QoS (4 files de sortie par port, champ priorité (*Prio*) dans la trame), limitation adaptative du débit.
- Fonctions de sécurité pour l'ensemble du réseau.

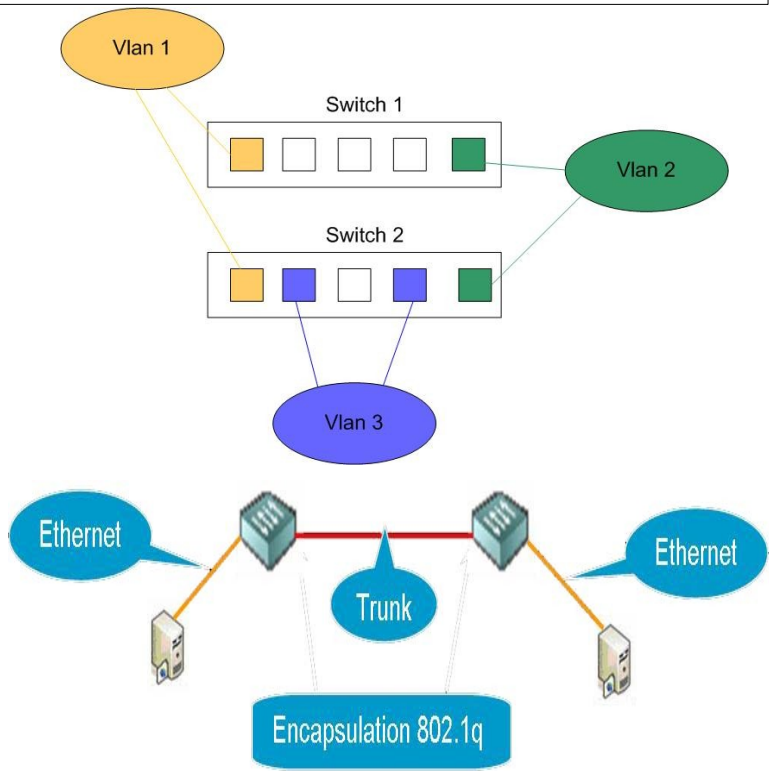
Principe de fonctionnement

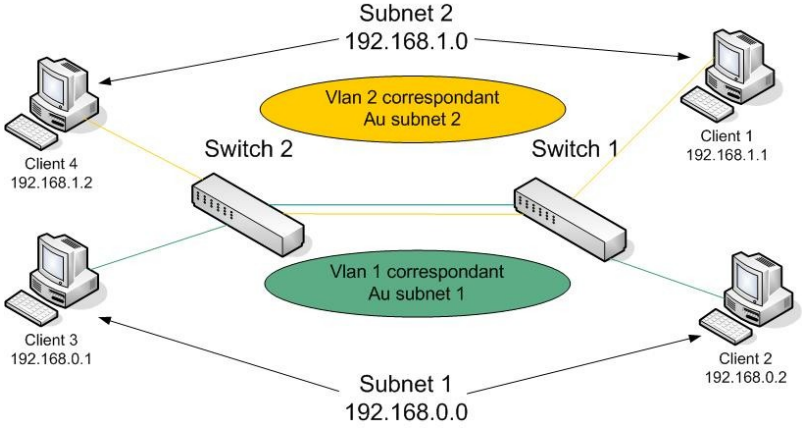
- Un switch2-3 permet de répartir les stations qui lui sont connectées en plusieurs réseaux IP **virtuellement** indépendants (VLANs) :
  - Un VLAN fonctionne comme un réseau local Ethernet : les stations d'un même VLAN font partie du même réseau Ethernet (et donc du même réseau IP).
  - Chaque VLAN étant un réseau IP, il a une adresse de réseau IP et un espace d'adresses IP avec une @IP par station qui en fait partie, **plus une @IP pour le switch2-3**.
  - Le switch2-3 utilise la **commutation Ethernet** pour faire communiquer les stations d'un même VLAN (table de commutation : N° de ports du switch ↔ adresses MAC).
  - Pour les échanges entre stations de VLANs différents, le switch2-3 utilise le **routage IP** (table de routage, @ IP).
- Avantages : administration centralisée des réseaux, évolutivité plus grande, isolation des trafics (sécurité).

Types de VLANs

Source : **http://www-igm.univ-mlv.fr/~dr/XPOSE2006/SURZUR-DEFRANCE/vlan.html**

- VLAN de niveau 1 : répartition des stations dans les VLANs en fonction des ports des switch2-3 :
  - Mise en place simple sauf si les VLANs sont sur plusieurs switchs (utiliser 802.1q).
  - Très bonne sécurité.
- VLAN de niveau 2 : chaque VLAN est défini par la liste des @MAC des stations :
  - Configuration centralisée entre switchs.
  - Sécurité moyenne (usurpation d'@MAC)
- VLAN de niveau 3 : chaque VLAN est défini par son @IP de réseau :
  - Appartenance automatique d'une station par son @IP (mais plus lent car niveau 3).
  - Sécurité faible (usurpation d'@IP).

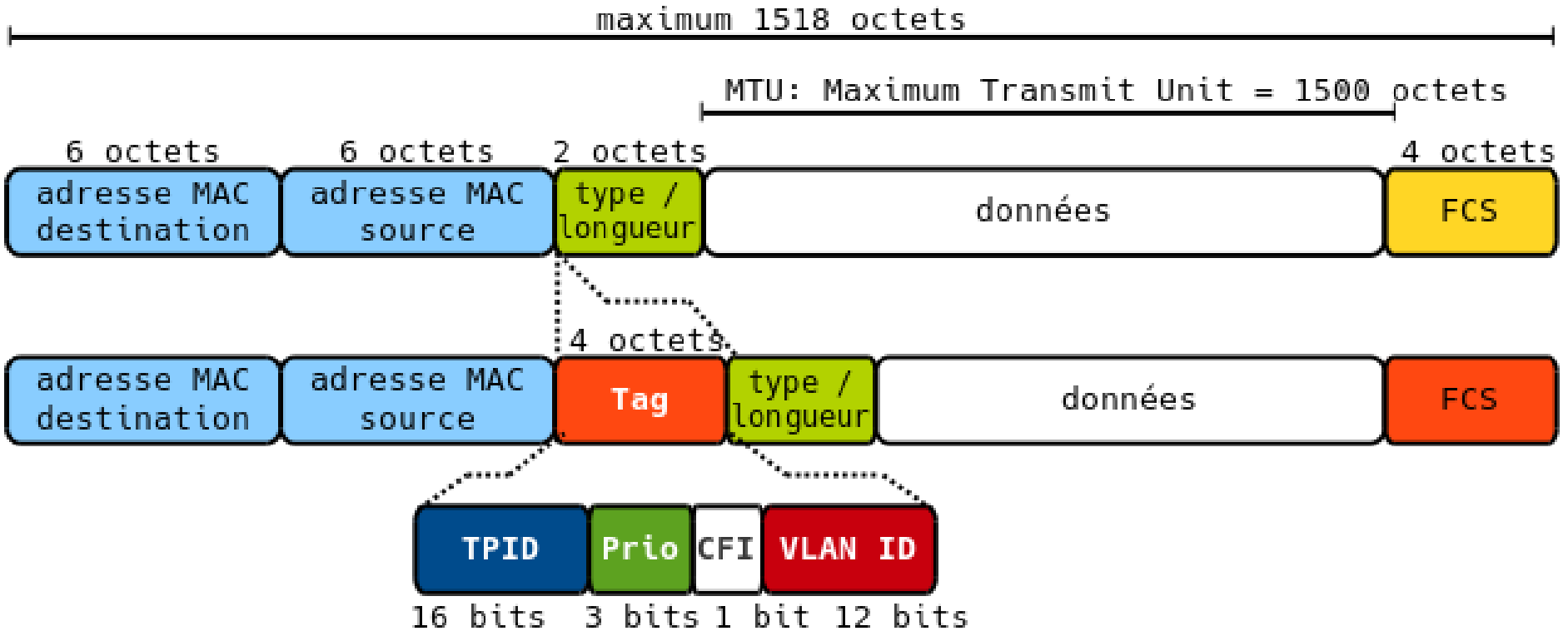




Répartition des stations dans les VLANs

- Répartition statique de niveau 1 : un VLAN est défini comme l'ensemble des stations reliées par un **ensemble donné de ports** d'un switch2-3 :
  - Les stations d'un même port font toujours partie du même VLAN.
  - Les trames échangées entre les stations d'un même VLAN sont des trames Ethernet standard.
- Répartition dynamique de niveau 1 avec un **identifiant**, dans le cas d'un inter-réseau formé de plusieurs switch2-3 :
  - Les ports des switch2-3 sont affectés chacun à un VLAN.
  - Les stations d'un même VLAN sont librement réparties.
  - Chaque VLAN est identifié par un VLAN ID (VID) sur 12 bits.
  - Le protocole 802.1q est activé entre les switch2-3 pour que les trames échangées soient des « tagged frames » comprenant dans l'en-tête le champ d'identification de VLAN (VID) permettant aux switch2-3 de rediriger correctement les trames.

Format de trame 802.1q

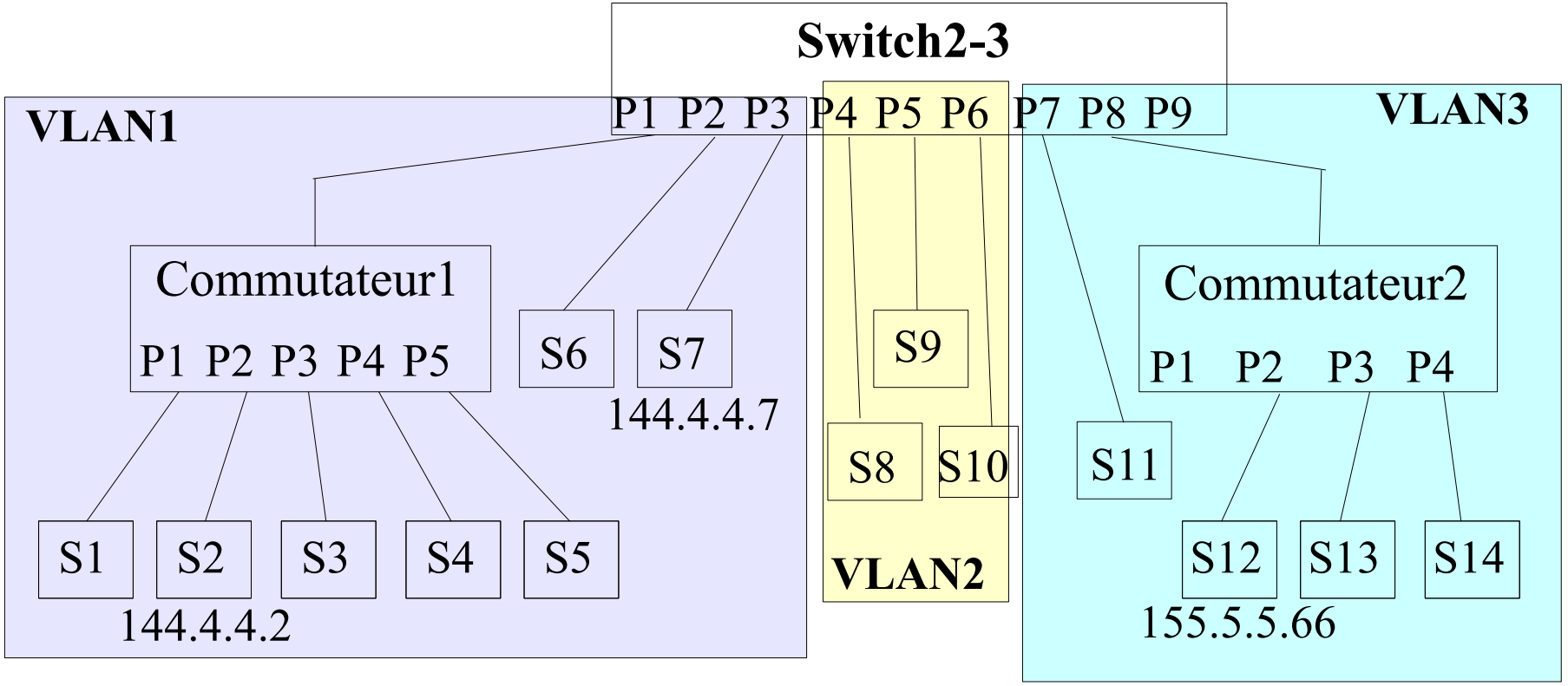


Le champ **TPID** a pour valeur 0x8100 pour identifier le mode « tagged trame » du protocole 802.1q, et différencier les trames Ethernet simples qui ont juste le champ **Type**. Le champ **Prio** (priorité) permet de gérer des flux différentiés pour la mise en place de la QoS (qualité de service).

https://inetdoc.net/articles/inter-vlan-routing/inter-vlan-routing.vlan.html#inter-vlan-routing.vlan.dot1q

Voir aussi : https://en.wikipedia.org/wiki/IEEE_802.1Q

Mise en œuvre de VLANs
Exemple de configuration statique



Trois VLANs :

VLAN1 : (P1, P2, P3) @IP:144.4.4.0/24

VLAN2 : (P4, P5, P6) @IP:155.5.5.32/27

VLAN3 : (P7, P8, P9) @IP: 155.5.5.64/26

Adresses du switch2-3

- C'est un routeur IP : il a donc autant d 'adresses IP que de réseaux VLAN IP qu'il définit :
  - @IP dans le VLAN1 : 144.4.4.32
  - @IP dans le VLAN2 : 155.5.5.48
  - @IP dans le VLAN3 : 155.5.5.65

- À ces adresses IP sont associées des adresses MAC :
  - @MAC (P1, P2, P3) : 00:0D:29:E3:63:44
  - @MAC (P4, P5, P6) : 00:0D:29:E3:63:45
  - @MAC (P7, P8, P9) : 00:0D:29:E3:63:46

Tables du switch2-3

- **Table de commutation** utilisée pour tous les échanges entre stations d'un **même** VLAN (équivalente à 3 tables de commutation).

@MAC dest	n° port
@MAC S1 à S5	P1
@MAC S6	P2
@MAC S7	P3
@MAC S8	P4
@MAC S9	P5
@MAC S10	P6
@MAC S11	P7
@MAC S12 à S14	P8

- **Table de routage** pour les autres échanges :

Destination	Mask	Gateway	Interface
144.4.4.0	255.255.255.0	0.0.0.0	eth0
155.5.5.32	255.255.255.224	0.0.0.0	eth1
155.5.5.64	255.255.255.192	0.0.0.0	eth2

Tables de routage des stations

- Les tables de routage des stations du VLAN1 sont de la forme :

Destination	Mask	Gateway	Interface
144.4.4.0	255.255.255.0	0.0.0.0	eth0
0.0.0.0	0.0.0.0	144.4.4.32	eth0

- Les tables de routage des stations du VLAN2 sont de la forme :

Destination	Mask	Gateway	Interface
155.5.5.32	255.255.255.224	0.0.0.0	eth0
0.0.0.0	0.0.0.0	155.5.5.48	eth0

- Les tables de routage des stations du VLAN3 sont de la forme :

Destination	Mask	Gateway	Interface

Fonctionnement du switch2-3 : commutation ou routage ?

- Cas1: **S2** envoie un paquet à **S7** :
  - Sa table de routage indique que le « gateway » est elle-même.
  - S2 envoie donc directement une trame dont l'adresse destination Ethernet est l'adresse de **S7**.
  - Le switch2-3 reçoit une trame dont il n'est pas le destinataire : il utilise donc sa table de commutation pour envoyer cette trame sur le port 3 où est situé **S7**.
- Cas2 : **S2** envoie un paquet à **S12** :
  - Sa table de routage lui indique que le « gateway » est le switch2-3 d'adresse IP 144.4.4.32.
  - S2 envoie donc une trame Ethernet dont l'adresse destination est l'adresse MAC du switch2-3 sur le réseau 144.4.4.0.
  - Le switch2-3 va faire appel à sa table de routage IP pour pouvoir acheminer ce paquet vers **S12**.