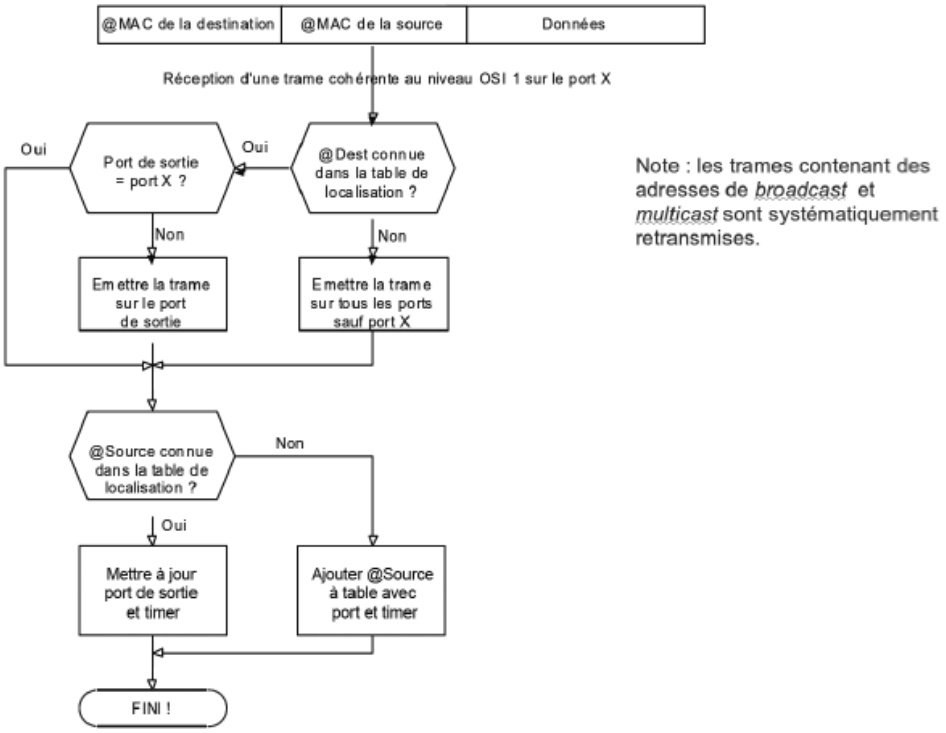
Segmenter un LAN (OSI2)

1. Révisions

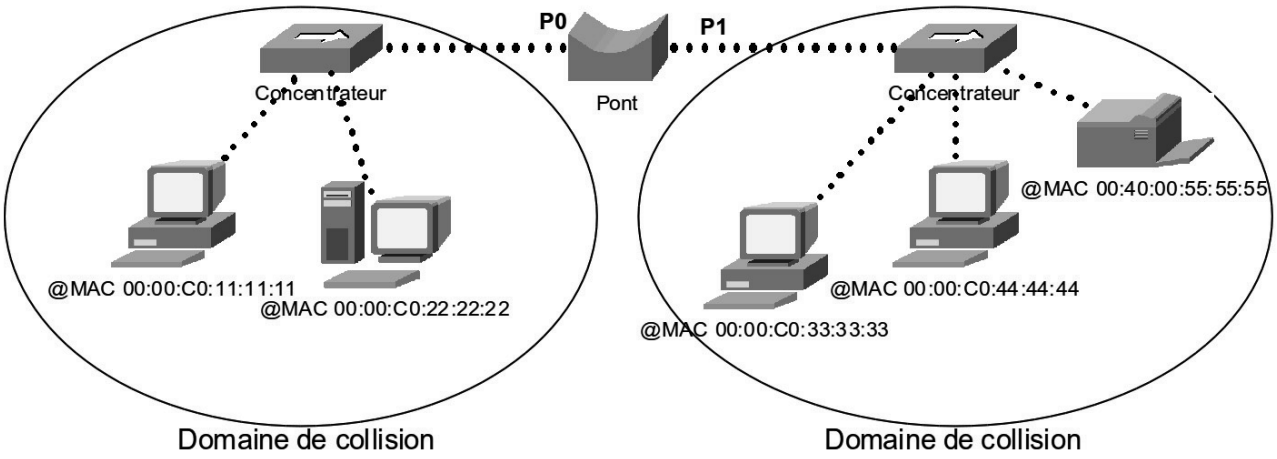
Au niveau OSI2, nous sommes dans le domaine des trames, des topologies, des méthodes d'accès au média et des adresses physiques. Les appareils agissant à ce niveau pourront donc analyser les trames et les traiter mais sans « comprendre » le contenu encapsulé provenant des couches supérieures. Contrairement au niveau 1, différents paramètres permettent de gérer un certain degré de sécurité car ces technologies sont sensibles et font partie des cibles favorites des gens mal intentionnés.
Un des intérêts de la segmentation d'un LAN est l'aspect sécuritaire. Divers dispositifs permettent cette segmentation : le pont et le switch notamment.

Un pont est un appareil doté d'au moins deux ports réseau. Derrière chaque port se trouve un segment de réseau. Une trame reçue traversera le pont uniquement si la destination se trouve dans l'autre segment. Pour ce faire, il analyse toutes les trames reçues et à partir des adresses MAC qu'elles contiennent, il gère de façon transparente une **table de localisation** mettant en correspondance adresse MAC / port du pont.
Lorsque le pont est mis en service, il ne connaît aucune adresse MAC. Il va mettre en oeuvre un processus d'apprentissage afin de savoir quel appareil se trouve sur quel segment.

On peut représenter ce processus de constitution de la table de localisation grâce à l'organigramme suivant :



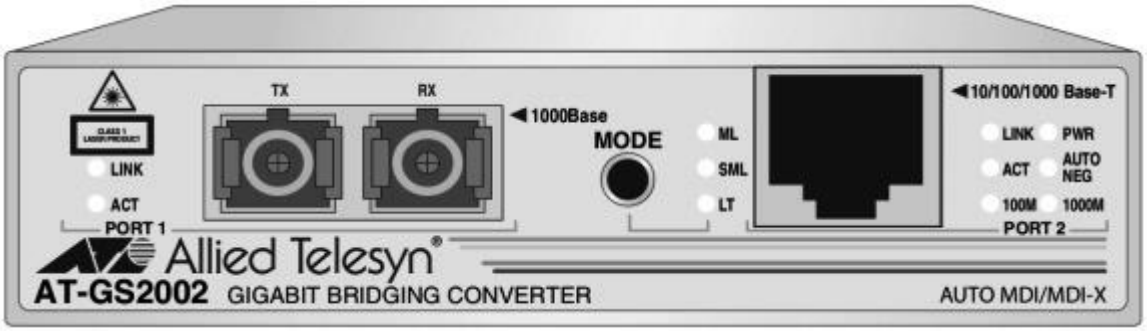
Le pont isole deux domaines de collision. L'ensemble constitue toutefois un domaine de diffusion (broadcast) unique (i.e. les collisions ne sont pas propagées mais les broadcasts le sont). Examinons la figure suivante :



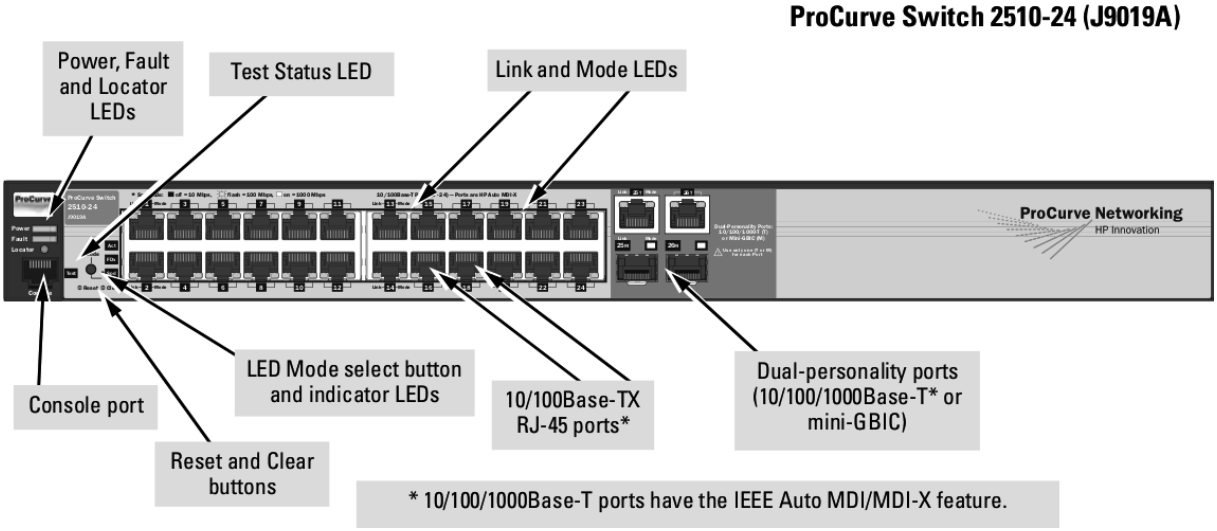
L'examen de ce réseau nous permet d'établir la table de localisation du pont :

P0		P1	
@ MAC	Timer (TTL)	@MAC	Timer (TTL)
00 :00 :C0 :11 :11 :11	64	00 :00 :C0 :33 :33 :33	2
00 :00 :C0 :22 :22 :22	121	00 :00 :C0 :44 :44 :44	15
		00 :40 :00 :55 :55 :55	110

Le TTL ou Time To Live nous rappelle que ces données sont découvertes automatiquement par l'appareil mais qu'elles ne seront conservées que pendant un laps de temps afin de gérer les modifications du réseau comme le déplacement d'une machine.
Extérieurement, l'appareil ressemble à un répéteur.
Ici un pont gigabit fibre optique/paire torsadée (10/100/1000) :

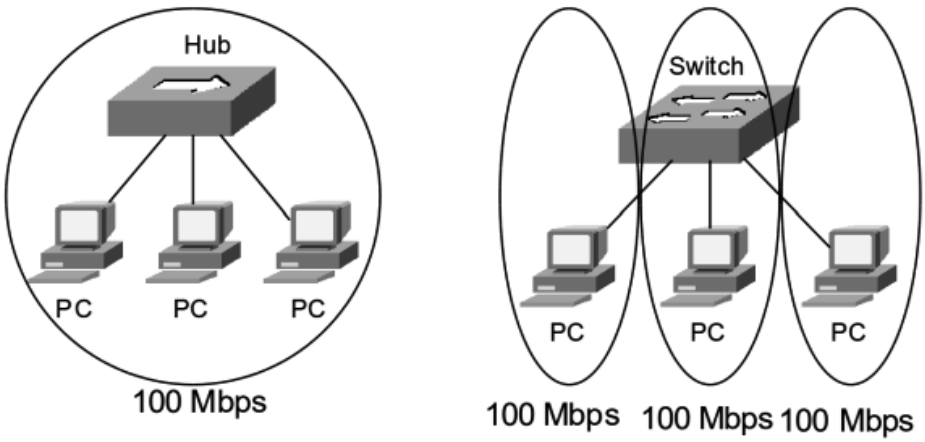


De la notion de pont, on peut généraliser à celle de commutateur (switch) en disant qu'il s'agit d'un « pont multiport ». Observons par exemple un switch HP :



On distingue deux grandes familles de switches : **administrable** ou **non administrable**.
Les commutateurs non administrables n'ont aucune interface de configuration, ils sont « plug and play » en quelque sorte. On connecte les machines, on l'allume et c'est tout. Il fait son travail sans rien demander à personne. Vous vous doutez que ces modèles ne nous intéressent pas du tout. D'autant plus que nous allons voir que le principe de la table de localisation pose un sérieux problème de sécurité qu'il n'est pas possible de traiter avec ces appareils.

Pour terminer sur ces généralités, rappelons que contrairement aux répéteurs/concentrateurs, les ponts/commutateurs présentent l'avantage essentiel de mieux répartir la bande passante et d'améliorer la sécurité en isolant une partie du trafic réseau :



C'est pourquoi ces appareils sont universellement répandus dans les réseaux d'entreprise.

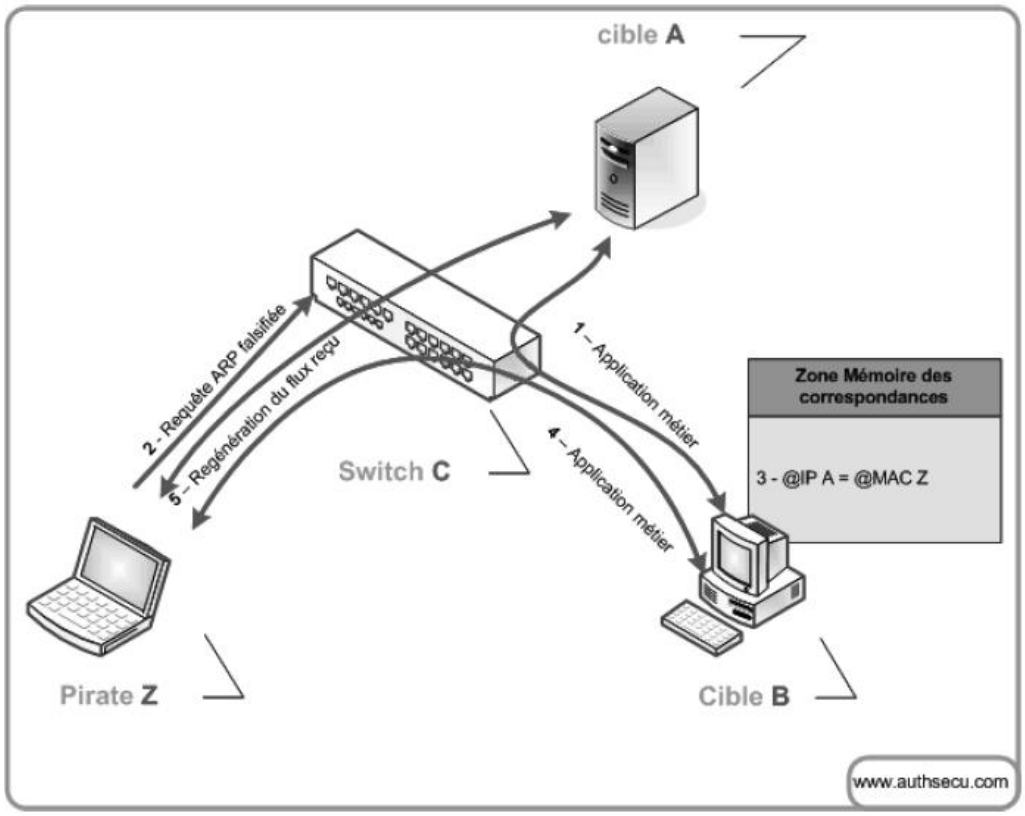
Nous allons maintenant voir les 4 grandes fonctionnalités des commutateurs avec un approfondissement des configurations et surtout la sécurisation :

- table de localisation ;
- VLAN ;
- liens redondants ;
- agrégation de liens.

2. Protocole ARP

Avant cela, parlons du protocole ARP et de son dégré de sécurité. Absolument tous les réseaux Ethernet/TCP IP (donc à peu près tous les réseaux locaux de la terre) utilisent le protocole ARP (qui se trouve à cheval entre les couches 2 et 3 du modèle OSI). Or ce protocole comporte intrinsèquement une faiblesse que dans certains cas nous pourrons combattre avec les commutateurs.

Pour rappel, le protocole ARP permet de faire la résolution d'une adresse IP en adresse physique MAC, par contre sans aucune vérification. Observons la figure suivante :



En fonctionnement normal, la machine B qui dialogue avec la machine A devrait disposer dans son cache ARP de l'information suivante :

@IP A	@ MAC A

La machine Z va fabriquer une fausse correspondance et va l'envoyer à la machine B qui, bêtement, va mettre à jour son cache ARP :

@IP A	@ MAC Z

Ainsi, tous les paquets que B veut envoyer à A iront à Z car l'adresse MAC des trames sera erronée. Afin que cela passe inaperçu, après avoir soigneusement gardé une trace des données, Z transférera quand même les trames à A.
Ce genre de méthode d'attaque porte divers noms comme *ARP Spoofing*, *ARP Poisonning* ou encore *ARP Redirect*. Le résultat est connu sous le nom de « *man in the middle* » lorsqu'il y a retransmission sinon cela s'appelle un déni de service, puisque les paquets à destination d'une machine sensible (en général un routeur ou un serveur) tombent dans *un trou noir.*

Prévention
Cette attaque est relativement facile à mettre en oeuvre car de nombreux outils existent comme arpspoof. Mais comment s'en prémunir et limiter les risques ?

Comme toujours, il n'y a pas de solution miracle mais on peut agir à différents niveaux.
Premièrement, sur les machines sensibles (comme la machine A de la figure précédente), on peut utiliser un outil comme arpwatch qui détecte les modifications de couples IP/MAC et alerte l'administrateur.
Lorsque l'on veut protéger un certain nombre (réduit) de machines, on peut forcer la correspondance MAC/IP avec une commande qui l'enregistrera de façon statique dans le cache ARP. Du coup, les mises à jour dynamiques seront ignorées. Cela est relativement facile dans un domaine Windows via l'exécution de scripts à l'ouverture des sessions (exemple sous Linux mais valable sous Windows) :

```
$ sudo arp -s 192.168.1.36  00:18:e7:66:c2:77
$ arp -n
Address         HWtype      HWaddress           Flags Mask    Iface
192.168.1.36    ether       00:18:e7:66:c2:77   CM            eth0
192.168.1.1     ether       00:18:e7:66:c2:62   C             eth0
```

Enfin, si nos switches sont suffisamment intelligents, des technologies basées sur le *DHCP Snooping* lui permettront de vérifier pour chaque trame reçue la cohérence des adresses MAC/IP par rapport à une table constituée lors du transfert des requêtes DHCP. Par exemple, le serveur DHCP a attribué une adresse IP à une machine, le switch a vu passer la requête et l'a mémorisée :

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress          Lease(sec)  Type            VLAN  Interface
------------------  -------------      ----------  -------------   ----  --------------
00:1C:23:14:12:27  192.168.51.10 69    1130        dhcp-snooping   11    FastEthernet0/1
Total number of bindings: 1
```

Ensuite, on active le DAI (*Deep Packet Inspection*) et le switch contrôlera toutes les trames.

3. La table de localisation

3A. Présentation du risque

Nous avons vu en introduction que la table de localisation est constituée automatiquement par le commutateur. D'un côté, c'est formidable, il apprend tout seul et améliore le débit en évitant du trafic inutile et la sécurité puisque tout le monde ne reçoit pas toutes les trames comme dans un environnement de type « concentrateur ».

Comme toute chose, les commutateurs ont une certaine quantité de mémoire qu'ils peuvent allouer à la table de localisation. Elle a donc une taille limitée. Par exemple, le switch Cisco 2960 peut gérer jusqu'à 8000 adresses MAC (source Cisco).

Une personne mal intentionnée peut polluer cette table avec de fausses informations (Déni de Service) ou elle peut également la saturer (MAC Flooding).

3B. Prévention

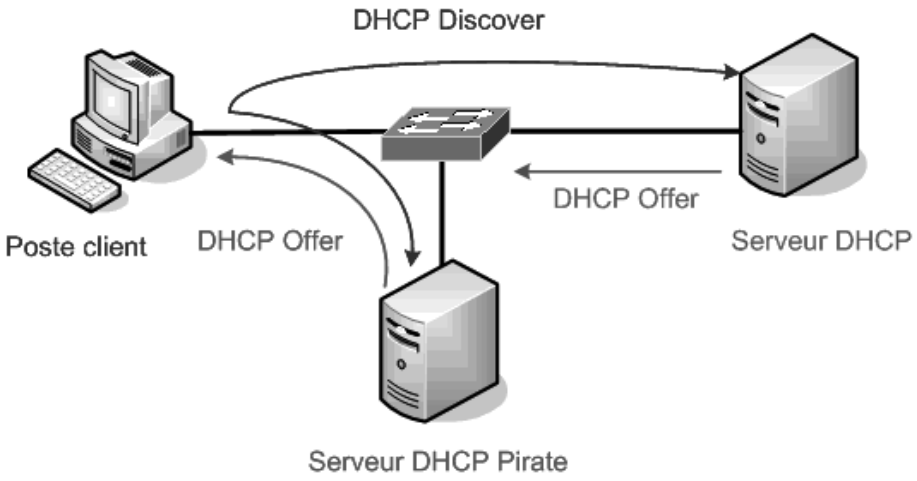
Nous allons donc intervenir au niveau du switch pour limiter le nombre d'adresses MAC derrière chaque port. En effet, dans un environnement moderne, il n'y a qu'une carte réseau derrière chaque port de switch. On peut donc associer manuellement une adresse MAC à un port. Une autre méthode plus souple, consiste à expliquer au commutateur que la première adresse découverte sera la seule à autoriser. Enfin, il peut arriver que les switches au contact des machines ne soient pas administrables. Dans ce cas, il faut remonter au switch fédérateur et configurer une limite d'adresses MAC par port.

4. Le DHCP

Quoi DHCP ? Mais c'est pas de l'OSI 2 ça ! Oui, mais supposons qu'un petit farceur mette en route un serveur DHCP pirate sur le réseau délivrant des adresses ridicules aux machines. Quel est le résultat ? Déni de service généralisé. Heureusement, le commutateur a une solution !

Déjà évoquée : il s'agit du DHCP Snooping. Nous configurons le port du switch relié au vrai serveur DHCP comme un port de confiance. Ainsi toutes les propositions de bail émanant des autres ports seront rejetées. On peut même limiter le nombre de requêtes par seconde autorisé (pour bloquer les personnes qui cherchent à saturer le serveur DHCP).

Le principe du *DHCP Spoofing* :



L'antidote ou DHCP Snooping :

Seul le port 2 est considéré de confiance (trust) pour répondre à des requêtes DHCP.

Exemple de configuration (non démontrable avec Packet Tracer) :

1. Switch(config)# ip dhcp snooping
2. Switch(config)# ip dhcp snooping vlan 3 15
3. Switch(config)# ip dhcp snooping information option
4. Switch(config)# interface fastethernet0/0
5. Switch(config-if)# ip dhcp snooping trust
6. Switch(config-if)# ip dhcp snooping limit rate 50

Ce qui signifie :
1. On active le DHCP snoooping.
2. On définit sur quel(s) VLAN le *DHCP snooping* s'appliquera.
3. On active l'option 82 du protocole DHCP car le *DHCP snooping* en a besoin.

Enfin, on définit une (éventuellement plusieurs) interface de confiance sur laquelle se trouve le serveur DHCP.
4. On rentre dans la configuration de l'interface.
5. On la place en « trust ».
6. On définit éventuellement un nombre de requête maximal par seconde autorisé.

On pourra par la suite consulter l'état de la configuration :

```
Switch# show ip dhcp snooping
DHCP Snooping is configured on the following VLAN:    3 15
Insertion of option 82 information is enabled.
Interface                Trusted                 Rate limit (pps)
---------                -------                 ----------------
FastEthernet0/0          yes                     50
```

Et la table d'affectation découverte par le switch :

```
Switch# show ip dhcp snooping binding
MacAddress          IP Address      Lease (seconds)   Type          VLAN    Interface
--------------      ----------      ----------------  ---------     --------  --------------
0000.0100.0201      10.0.0.1        1600              dynamic       100     FastEthernet2/1
```

5. Le protocole CDP

Par défaut, les appareils Cisco sont configurés pour diffuser un maximum d'informations sur toutes ses interfaces.

CDP pour *Cisco Discovery Protocol* est un protocole propriétaire, parfois implémenté sur des appareils non Cisco, et qui sert à partager avec les éléments actifs voisins des informations sur leurs caractéristiques (adresses IP, version d'IOS, informations sur les VLAN, etc.).

Différents logiciels comme cdpsnarf permettent à n'importe qui sur votre réseau de récupérer ces informations qui sont diffusées en multicast toutes les 60 secondes (par défaut) en se faisant passer à loisir comme un commutateur, un routeur, un téléphone IP, etc.

Même si CDP peut être complètement désactivé, une bonne pratique, que nous mettrons en oeuvre dans l'atelier, est de limiter CDP aux interfaces réseau de « confiance » comme par exemple, les liens inter-switches sur lesquels aucune machine n'est connectée.

Remarque : IOS Internetwork Operating System est l'OS de Cisco.

6. Le Spanning Tree

Le Spanning Tree est un algorithme exécuté par les switches et les ponts pour empêcher les boucles dans le réseau local. Ces boucles peuvent être volontairement créées afin d'introduire de la redondance dans le réseau et d'être en mesure de gérer la coupure de certains liens.

Spanning Tree Protocol (STP) et ses variantes comme RSTP (Rapid Spanning Tree Protocol) sont des mécanismes de détection de boucle dans le réseau (boucle physique ou boucle logique, par exemple par VLAN). Le port détecté et élu comme étant sur le chemin redondant passe en mode bloqué jusqu'à la détection d'un problème. STP est bien souvent activé par défaut sur tous les ports d'un commutateur et, autre caractéristique intéressante, durant le processus d'élection STP, les ports concernés sont inactifs : il est impossible d'envoyer ou de recevoir des trames Ethernet.

Le problème avec ce protocole c'est que, comme pour ARP par exemple, les switches se font mutuellement confiance. Aucun mécanisme d'authentification n'existe. Ainsi, si un « switch » (en fait un simple PC avec le bon logiciel) est introduit dans le réseau, il peut diffuser de fausses annonces, devenir la racine de l'arbre (tree) constitué par les commutateurs et donc récupérer du trafic réseau, provoquer des dénis de services, etc.

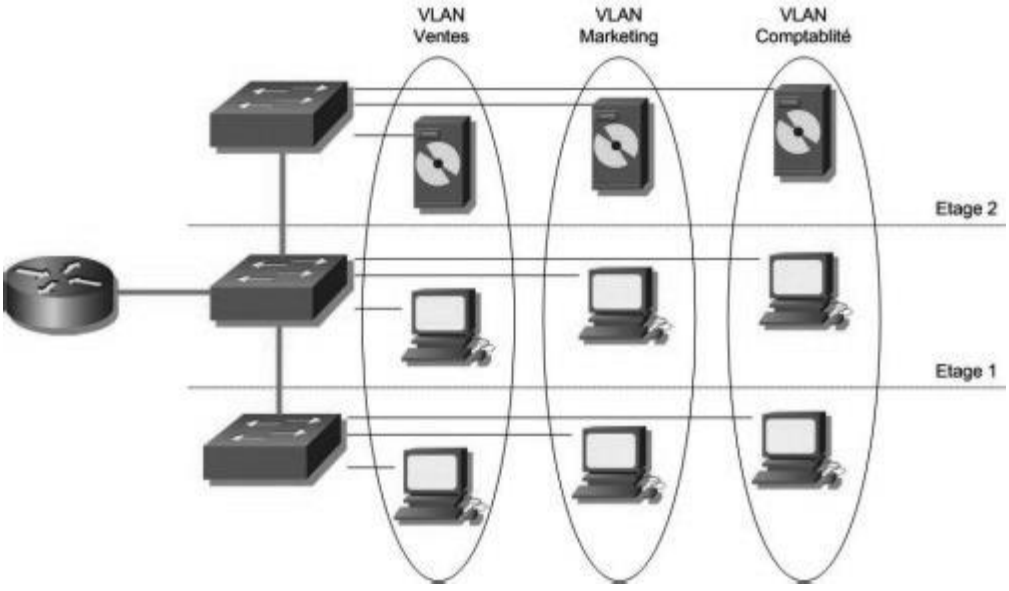
Une bonne idée consiste à ne pas faire de boucle au niveau OSI 2, à ne pas utiliser STP ; et à laisser gérer la redondance des liens par des routeurs.

Voici une parade (non démontrable sous PacketTracer) : refuser les mises à jour STP (bpdu) arrivant sur les interfaces qui ne sont pas des liens inter-switch :

Switch(config-if)# spanning-tree bpduguard enable

7. Les VLAN

Les VLAN (Virtual Local Area Network) permettent de regrouper des machines dans des réseaux indépendants, sans avoir à tenir compte de leur emplacement physique sur le réseau. Soit le schéma :



Le commutateur est au coeur d'une architecture de VLAN. Dans l'exemple ci-dessus, les machines du réseau ont été regroupées dans 3 VLAN distincts. Une machine dans un VLAN ne peut joindre une machine située dans un autre VLAN (sauf à passer par le routeur).

Les avantages des VLAN sont :

• amélioration de la sécurité en isolant des groupes de machines ;
• amélioration des performances du réseau car basés sur la commutation ils limitent les domaines de diffusion ;
• permettent une organisation virtuelle et une gestion simplifiée des ressources en autorisant des modifications logiques ou géographiques gérées via la console plutôt que dans l'armoire de brassage ;
• selon le type de VLAN, un poste déplacé retrouve les mêmes ressources avec ou sans reconfiguration du VLAN.

Les différents niveaux de VLAN :

- VLAN de niveau 1 (ou VLAN par port) : Il faut ici inclure les ports du commutateur qui appartiendront à tel ou tel VLAN. Cela permet entre autres de pouvoir distinguer physiquement quels ports appartiennent à quels VLAN.
- VLAN de niveau 2 (ou VLAN par adresse MAC) : Ici l'on indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN, cette solution est plus souple que les VLAN de niveau 1, car peu importe le port sur lequel la machine sera connectée, cette dernière fera partie du VLAN dans lequel son adresse MAC sera configurée.
- VLAN de niveau 3 (ou VLAN par adresse IP) : Même principe que pour les VLAN de niveau 2 sauf que l'on indique les adresses IP (ou une plage d'IP) qui appartiendront à tel ou tel VLAN.

7A. Les bonnes pratiques

Tout switch Cisco dispose par défaut d'un seul VLAN qui porte le numéro 1 et qui concerne tous les ports. Si vous n'implémentez pas de VLAN, c'est parfait, ne touchez à rien. Sinon, ce VLAN 1 (qui ne peut pas être désactivé) ne doit pas être utilisé, ni pour véhiculer de données utilisateur, ni pour l'administration. Le VLAN 1 est le **vlan natif**. Son rôle est particulier car il transporte tous les protocoles implémentés par le switch (STP, DTP, VTP) et est aussi utilisé pour transférer tout le trafic qui n'est pas compatible avec IEEE802.1q (par exemple, si le réseau dispose de switches anciens). Si ce type de trafic n'est pas présent dans votre réseau, autant affecter au VLAN natif un numéro de VLAN inutilisé.

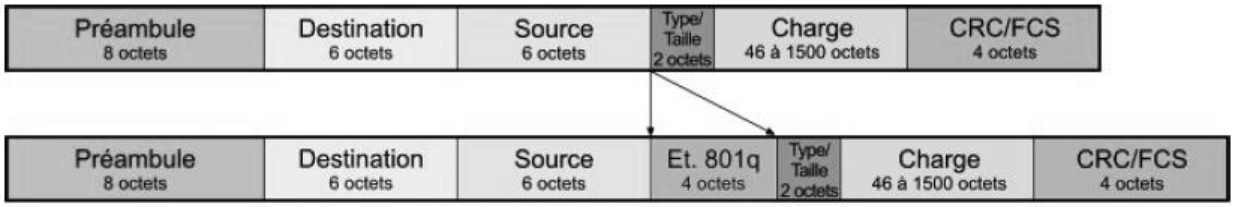
En résumé, il est conseillé de :

• placer les données utilisateurs dans d'autres VLAN que le 1 ;
• créer un VLAN spécifique pour l'administration des switches ;
• diriger le VLAN natif dans un VLAN « bidon » ;
• limiter le trafic sur le « trunk » aux seuls VLAN existants.

7B. Les risques

Un VLAN est un domaine de diffusion Ethernet logique. L'utilisation des VLAN permet de rationaliser l'utilisation des ports physiques des commutateurs et de rendre la gestion du réseau d'entreprise plus simple, puisque pour placer un utilisateur dans un réseau particulier, il suffit de placer le port physique auquel il est connecté dans le bon VLAN. Cette notion de

VLAN peut-être exportée d'un commutateur à un autre en utilisant des liens spécialisés appelés *trunks.* Ces derniers véhiculent des trames Ethernet au format 802.1q : elles possèdent un champ supplémentaire indiquant à quel VLAN elles appartiennent. La figure ci-dessous montre la différence entre une trame « classique » IEEE802.3 et une trame modifiée par l'insertion d'un *tag* IEEE802.1Q :



Où L'étiquette IEEE 802.1q est composée de :

- **TPID** *Tag Protocol Identifier* (16 bits) : 0x8100, valeur annonçant la charge IEEE 801.q
- **TCI** *Tag Control Identifier* (16 bits) :
  - **PCP** *Priority Code Point* (3 bits), priorité IEEE 802.1p
  - **CFI** *Canonical Format Indicator* (1bit), la valeur 0 correspond à une adresse MAC en format canonique
  - **VID** *VLAN Identifier* (12 bits), l'identifiant VLAN

Pour un attaquant, la possibilité, depuis un VLAN donné, d'envoyer du trafic dans un autre VLAN, de changer de VLAN ou, mieux, d'accéder à plusieurs VLAN choisis, présente un intérêt tout particulier, puisque cela lui permet *in fine* d'atteindre pratiquement toutes les machines du réseau sans passer par les points de routage et de filtrage mis en place entre les différents réseaux. Différentes attaques existent. La plus efficace consiste à modifier la configuration du port du switch auquel on est connecté, soit en attaquant le commutateur directement, soit en utilisant les protocoles DTP et VTP décrits par la suite.

Une autre attaque couramment évoquée est la double encapsulation 802.1q qui consiste à positionner deux fois les champs relatifs aux VLAN dans la trame Ethernet.
L'outil Scapy permet d'injecter du trafic dans de telles trames et, lorsque l'attaque fonctionne, d'établir une voie de communication à sens unique vers le VLAN cible. On pourra s'en servir pour déclencher une attaque de type *ARP poisonning* par exemple.
Cependant, des conditions très particulières doivent être réunies, ce qui est très rarement le cas, en particulier si on suit les conseils de déploiement des équipementiers.

Dynamic Trunk Protocol (DTP) : permet de transformer dynamiquement un port en mode hôte en un port en mode *trunk* : le port physique ne fait donc plus partie du VLAN mais permet de transporter un ensemble de VLAN.
Tous les ports d'un commutateur Cisco sont en mode DTP par défaut et le changement de l'état du port se fait par le simple envoi d'un message SNAP HDLC 0x2004 avec un outil comme Yersinia par exemple. Il est alors facile d'injecter des trames dans n'importe quel VLAN. En général les ports en mode *trunk* sont clairement identifiés et il est donc inutile de laisser tous les ports en mode automatique : la meilleure solution consiste à désactiver DTP sur l'ensemble du commutateur et configurer les ports « *trunks* » de manière statique.

VLAN Trunking Protocol (VTP) : permet une gestion centralisée des VLAN quand un ensemble de commutateurs sont interconnectés (via un *trunk).* Celui-ci facilite l'administration, car il n'est plus nécessaire de se connecter sur chacun d'eux pour créer un nouveau VLAN ou lui affecter des ports physiques, mais présente plusieurs failles de sécurité.
La plus simple à exploiter est le déni de service : l'injection aléatoire de messages VTP (SNAP HDLC 0x2003) avec Yersinia peut conduire au remplissage des ressources mémoire

ou au placement des hôtes dans de mauvais VLAN. S'il est possible de passer un port physique en *trunk* (si DTP n'est pas désactivé sur ce port) il devient alors facile d'injecter un message VTP pour reconfigurer les VLAN et les ports qui leur sont affectés : l'attaquant peut aisément se débrouiller pour changer de VLAN et de créer de fausses boucles.

Pour se protéger, la meilleure solution est de désactiver VTP (en activant le mode transparent) et se connecter sur les différents commutateurs pour modifier la configuration.
Un mot de passe permet de protéger son domaine VTP mais encore faut-il que celui choisi ne soit pas faible.

Ces différentes attaques s'appellent « VLAN Hopping ».

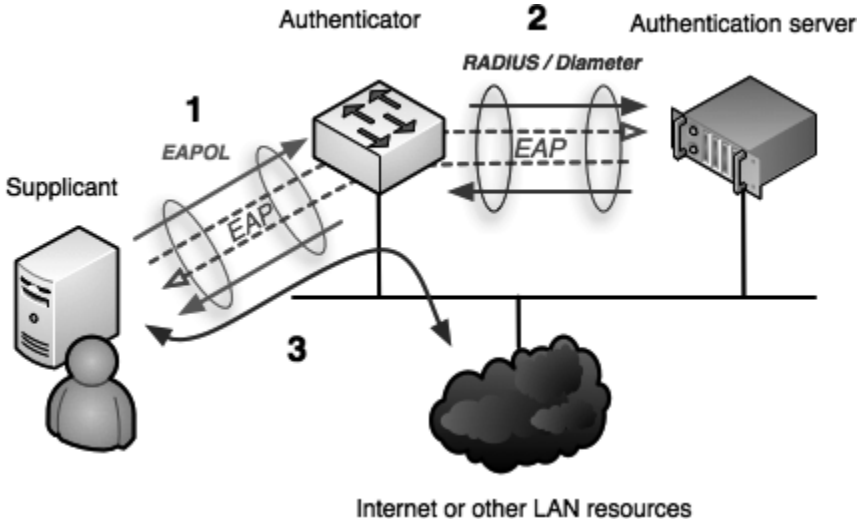
8. Agrégation de liens

Les switches et cartes réseaux conformes à la norme IEEE 802.1AX permettent de regrouper des liens Ethernet physiques afin d'améliorer le débit et la redondance. Cette agrégation peut se faire de switch à switch ou de PC à switch.

9. Sécurité sans-fil avec RADIUS

En s'appuyant sur le protocole EAP (Extensible Authentication Protocol) pour le transport des informations d'identification en mode client/serveur et sur un serveur d'identification, le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil.
Si un équipement réseau actif, tel qu'un commutateur réseau ou une borne Wi-Fi est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (PAE).
Indépendamment du type de connexion, chaque port se comporte alors comme une bascule à deux états : un état contrôlé en cas de succès d'identification et un état non contrôlé.

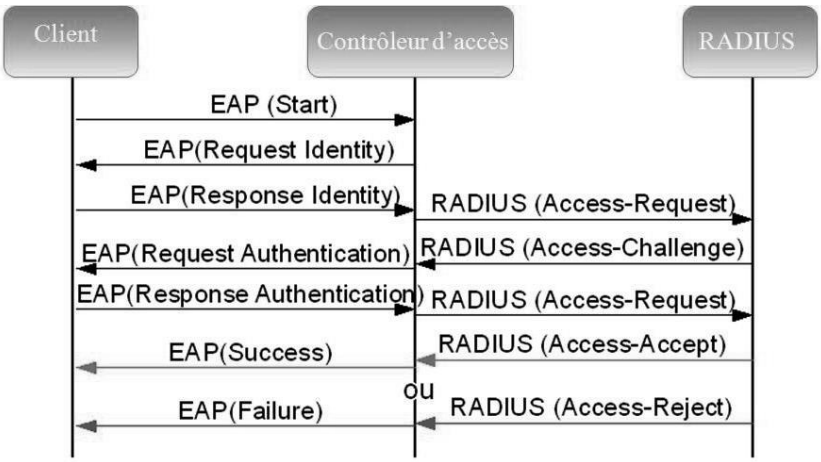
Nous avons donc 3 acteurs :



La mise en oeuvre d'un contrôle d'accès par port 802.1X nécessite l'activation du standard IEEE 802.1X sur :

• les commutateurs réseau et/ou les points d'accès sans fil (*authenticator*) ;
• chaque point terminal (*supplicant*) en EAP ordinateur hôte ;
• le serveur d'identification chargé de valider l'identité de l'utilisateur du port.

Les échanges entre les 3 se déroulent ainsi :

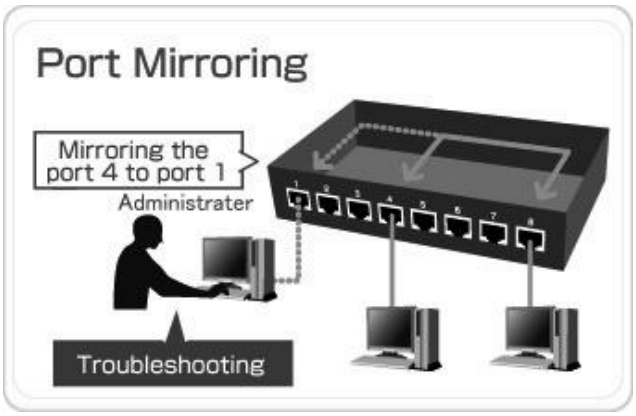


10. Port mirroring

Enfin une fonctionnalité positive ! Vous savez maintenant que dans un environnement commuté, une partie de trafic est invisible. Ainsi, si vous faites une capture de trame sur un port, vous ne verrez que 3 choses :
• le trafic qui vous concerne ;
• les trames de diffusion (broadcast) ;
• les trames de multi-diffusion (multicast).

Ceci peut être problématique si vous essayez de détecter des problèmes ou des tentatives d'intrusion, justement sans savoir précisément d'où elles viennent. Heureusement, les fabricants ont pensé à tout : le port mirroring.

Le principe est le suivant :



Tout le trafic est dupliqué sur un port « en lecture seule » à des fins d'analyse avec un logiciel adapté (type Wireshark ou détecteur d'intrusion IDS comme SNORT).