



Protocole 802.1Q & Attaques sur les VLAN

Equipe Projet:

*Sylvain ECHE (sylvain.eche@naema.org)
Constantin YAMKOUDOUYOU*

Sommaire

INTRODUCTION.....	3
1 Vlan selon la norme 802.1q.....	5
1.1 Modèle architectural.....	5
1.2 Architecture de la base de données de filtrage.	5
1.3 Typologies des vlan au sens 802.1q.....	6
1.4 Transmission dans un vlan.....	6
1.5 Principe de fonctionnement d'un switch 802.1Q	6
1.5.1 Relais et filtrage de trame	7
1.5.2 Règles de filtrage ingress.....	7
1.5.3 Règles de filtrage egress.....	7
1.5.4 Le process de forwarding	7
1.6 Structure des trames Ethernet étiquetées	8
1.6.1 Le champ Tag Protocol Identifier (TPID).....	8
1.6.2 Le champ Tag Control Information (TCI).....	8
1.6.3 Le champ Ethertype.....	9
1.6.4 Champ Embedded Source-Routing Information Field (E-RIF).....	9
2 Implémentation chez des équipementiers et systèmes d'exploitation libres.....	9
3 Mécanismes d'authentification dans les VLAN	10
4 La notion de Spanning Tree Protocol.....	11
5 La notion de trunk, VLAN natif et Dynamic Trunk Protocol.....	12
6 La notion de private VLAN (technologie CISCO).....	12
7 La notion de CDP (Cisco Discovery Protocol)	12
8 Attaques sur les VLAN	13
8.1 Attaque par MAC Flooding	13
8.2 Attaques par 802.1Q (standard), ISL (CISCO) tagging.....	15
8.3 Attaque par double encapsulation de 802.1 Q ou nested VLAN.....	15
8.4 Attaques ARP classiques	16
8.5 Attaques sur les privées LAN.....	17
8.6 Attaques par force brute multicast.....	17
8.7 Attaques sur le spanning tree.....	18
8.8 Random frame Stress Attack.....	19
9 Conclusion.....	20
10 Références	21

INTRODUCTION

Un VLAN¹ (Virtual Local Area Network) est un sous réseau de niveau 2² construit à partir d'une technologie permettant de cloisonner des réseaux par usage de filtres de sécurité. Cette technologie balise le domaine de broadcast auquel ces machines appartiennent de telle sorte que le trafic intra-domaine ne puisse pas être vu par des tiers n'appartenant pas à ce domaine de broadcast.

802.1Q est la norme de référence garantissant aujourd'hui une interopérabilité d'équipements provenant de divers constructeurs. Elle spécifie l'architecture des commutateurs, des bases de données de filtrage, la structure des trames, les traitements des paquets, la gestion des commutateurs et des topologies. C'est une des rares normes qui spécifie à la fois le comportement du matériel, les opérations (filtrage d'entrée, de sortie, forwarding) qui ont lieu dans un vlan, définit le codage et le contrôle des informations transportées par les trames, spécifie les règles qui régissent l'insertion et la suppression des informations de contrôle dans celles-ci.

Historiquement, il existe deux normes principales pour les vlan. La première est celle émanant des réseaux fédérateurs ATM permettant une interconnexion des réseaux virtuels ayant pour support les réseaux locaux classiques. Il s'agit des réseaux locaux émulsés LANE (LAN Emulation). Nous n'aborderons pas cette norme considérée comme aujourd'hui désuète par rapport à la norme 802.1Q. Ce document a une triple mission : donner un aperçu de l'état de l'art en matière de vlan à travers la norme 802.1Q, décrire l'implémentation de cette technologie dans des équipements de constructeurs, décrire également son implémentation sur des systèmes d'exploitation et enfin décrire des attaques connues à ce jour sur ces vlans.

Pour répondre aux objectifs précédemment énoncés, cette étude a été organisée en trois principaux chapitres. Un premier chapitre dans lequel il est question de la norme 802.1Q. Il s'agit d'une explication succincte de la norme à travers le concept de spanning tree, la notion de marquage de trame permettant d'introduire des balises supplémentaires de différenciation de trames et d'une description complète de la typologie de ces trames vlan.

Le deuxième chapitre est consacré à l'implémentation des vlans par quelques équipementiers du marché tels que CISCO et 3COM et aussi de l'implémentation sur des systèmes libres tels que GNU-Linux, FreeBSD.

¹ Par la suite nous noterons simplement vlan

^{2 2} Le concept de vlan de niveau trois existe, mais nous ne tenons pas compte de cette approche considérée comme désuète et moins répandue.

La dernière partie de ce document est consacrée aux vulnérabilités des réseaux vlan. Il s'agit d'attaques dont les principales sont celles par MAC flooding, 802.1Q, spanning tree et multicast.

Ce document a été rédigé dans le cadre d'un projet en partenariat avec Mr Melaine BROUDIC de France Télécom R&D. Il est perfectible et tout commentaire du lecteur pour son amélioration sera le bienvenu.

1 Vlan selon la norme 802.1q

Jusqu'à présent, plusieurs standards propriétaires permettaient la mise en place de cloisonnement logique de réseaux. C'est le cas par exemple du protocole ISL de cisco. Les spécifications du groupe 802.1q de l'IEEE ont pour but d'assurer l'interopérabilité d'équipements d'origines hétérogènes offrant des services de type réseaux locaux virtuels

1.1 Modèle architectural

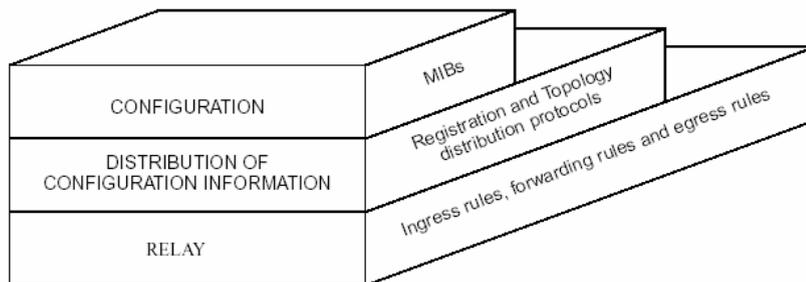


Figure 1 modèle architecturale vlan source 802.1Q

La norme présente un modèle à trois couches pour les vlans.

- La couche configuration qui permet d'indiquer comment sont associés les équipements aux différents réseaux vlan. Cette configuration pouvant s'opérer à partir de MIBs³ par le protocole SNMP ou des fichiers de configuration.
- La couche distribution/résolution qui permet aux switchs la résolution de chaque paquet par rapport à son vlan associé.
- La couche correspondance (relay) qui permet :
 - de déterminer l'unique vlan auquel les trames reçues appartiennent.
 - de déterminer sur quels ports du switch les trames doivent être transférées.
 - de modifier si nécessaire le format de la trame avant son envoi (ajout ou suppression d'étiquette, ...).

1.2 Architecture de la base de données de filtrage.

Trois aspects sont à prendre en considération pour l'architecture de la base des données de filtrage.

Pour certaines topologies de vlan il est nécessaire que tous les vlans aient connaissance de l'ensemble des adresses MAC réparties entre tous les vlans. Pour d'autres configurations cette connaissance doit être exclusive et les adresses Mac d'un vlan donné ne doivent pas être connues par un

³ Management Information Base

autre vlan. Enfin pour la troisième configuration cette connaissance importe peu.

Une combinaison de ces topologies de bases de données de filtrage peut être nécessaire selon les contraintes d'apprentissage de vlan exprimées dans un switch. Ce standard spécifie plus particulièrement une typologie de switches à même de supporter à la fois des bases de données de filtrage IVL et SVL . Cela permet d'associer M bases de données à N vlan.

1.3 Typologies des vlan au sens 802.1q.

La norme définit trois catégories de vlans:

- Les trames sans étiquette vlan (ou tag)
- Les trames dites prioritaires
- Les trames avec étiquette vlan (ou tag).

Les trames sans étiquette et les trames prioritaires ne comportent aucune information permettant d'identifier les vlans auxquels ils appartiennent. Ces trames appartiennent à des vlans spéciaux reliés à des ports physiques ou utilisant des extensions réservées à des équipementiers (3COM, CISCO..) dont la plupart ont participé à la rédaction du standard. Ces trames forment le vlan natif qui permet d'assurer l'interopérabilité avec un switch qui ne supporterait pas le 802.1q.

L'étiquette des autres trames comporte l'identifiant du vlan, le VID, (Vlan Identifier) auquel ils appartiennent.

1.4 Transmission dans un vlan.

Deux scénarii de transmission peuvent être définis dans un vlan. Une transmission de trames étiquetées et un mode sans étiquettes. Le mode avec étiquette suppose une capacité terminale d'interprétation des étiquettes pour les machines formant les vlans et aussi une capacité de forger des trames étiquetées destinées au switch. Dans le cas de la transmission de trame sans étiquettes, toute l'intelligence de traitement est supportée par le switch.

1.5 Principe de fonctionnement d'un switch 802.1Q

Trois principales opérations sont définies pour le fonctionnement d'un switch vlan. Il s'agit :

- Du relais et du filtrage de trames
- De la maintenance des informations de relais et de filtrage de trames
- De la gestion des deux types d'opérations

1.5.1 Relais et filtrage de trame

Le principe de retransmission et de filtrage des trames est illustré selon le schéma ci après.

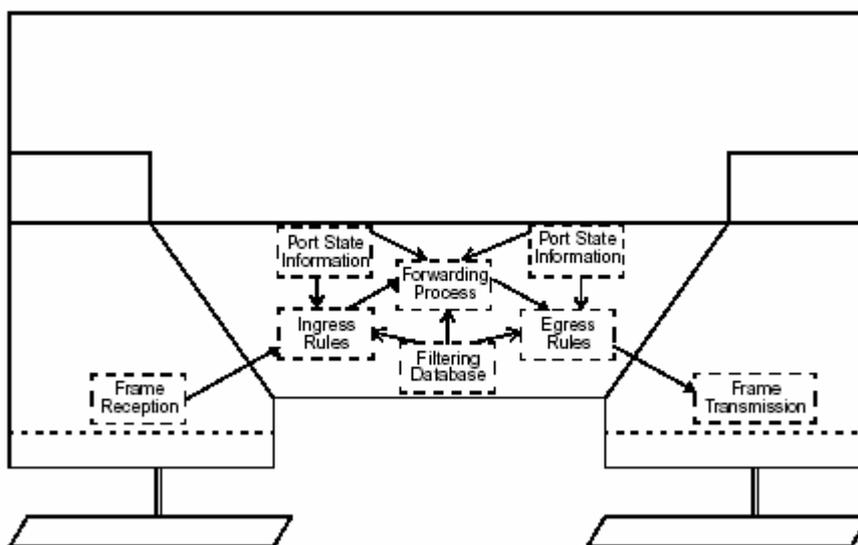


Figure 2 Architecture fonctionnelle de relais de trame 802.1Q

1.5.2 Règles de filtrage ingress

Ces règles s'appliquent à toutes les trames entrantes. La prise en compte de ces règles est spécifiée pour chaque port. Exemples de règles :

- Rejet de trames non « taggés » lorsque les règles de filtrage établies n'acceptent que les trames taggés
- Contrôle de l'appartenance à un vlan d'une trame reçue par comparaison aux données MAC stockées dans la base de données de filtrage.

1.5.3 Règles de filtrage egress

Idem que pour les règles de filtrage ingress et s'appliquent uniquement aux paquets en sortie.

1.5.4 Le process de forwarding

Le fonctionnement du switch 802.1Q est assimilable à celui d'un firewall. Les egress rules sont les règles de la table d'entrée applicable à tout paquet entrant.

Les « Port statement information » fournissent l'information sur la configuration de chaque port du switch.

La base de données de filtrage «filtering database » permet d'interpréter la sémantique de tous les paquets du réseau pour pallier au spoofing par exemple.

Le process de retransmission analyse l'ensemble de ces paquets selon les données émanant de la base de données de filtrage, des états de port et des règles ingress et egress et leur réserve ensuite le traitement approprié.

1.6 Structure des trames Ethernet étiquetées .

Les trames 802.1 Q diffèrent des trames classiques car elles possèdent :

- un entête supplémentaire inséré immédiatement entre les champs adresse source et destination.
- Un CRC en fin de trame, le FCS, après que le payload ait été rattaché a l'entête.

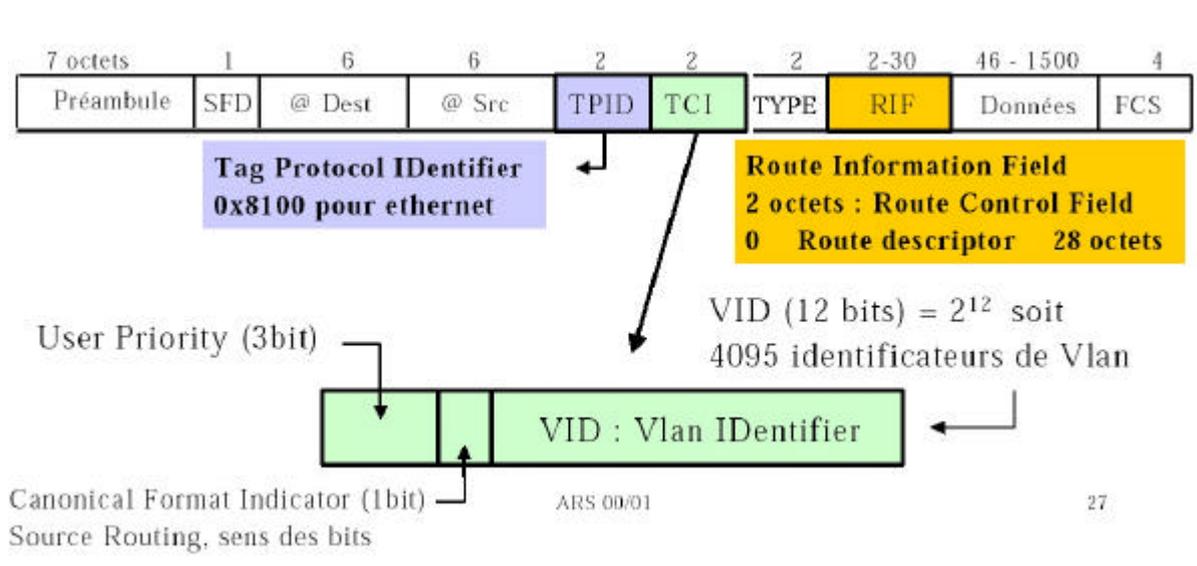


Figure 3 : format des trames Ethernet étiquetées

1.6.1 Le champ Tag Protocol Identifier (TPID).

Désigne le type de tag. Il permet par exemple au switch d'identifier la trame comme comportant un tag 802.1Q pour celle ayant un format Ethernet II / 802.3. Dans ce cas, cette valeur est égale à la constante hexadécimale 0x8100 codée sur deux octets.

1.6.2 Le champ Tag Control Information (TCI).

Ce champ a une longueur de 2 octets. Le premier champ de 3 bits, user_priority, permet de définir huit niveaux de priorité (voir ISO/IEC 15802-3 pour l'utilisation de ce champ). Lorsqu'il est positionné à 1, le bit CFI indique que les adresses MAC sont bien au format standard. Le champ VID de 12 bits désigne le VID (Vlan identifiant) auquel appartient la trame.

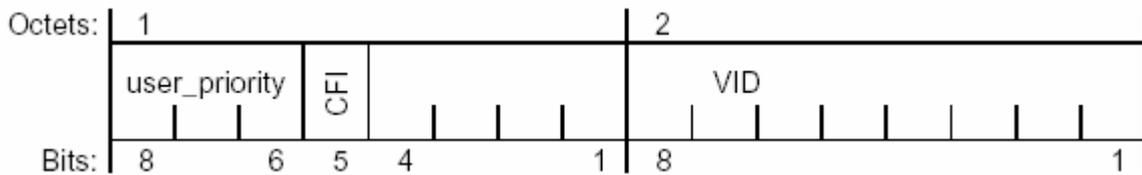


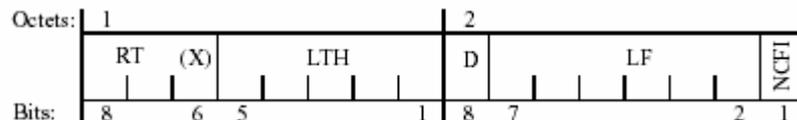
Figure 4 champ TCI dans un tag 802.1Q

1.6.3 Le champ Ethertype

Ce champ a déjà été décrit précédemment comme désignant le type de protocole de niveau 3. Il a été inséré dans le tag pour des questions d'ergonomie.

1.6.4 Champ Embedded Source-Routing Information Field (E-RIF)

Ce champ spécifie notamment les informations de routage (champ RT), ainsi que la longueur maximale des trames (champ LF).



2 Implémentation chez des équipementiers et systèmes d'exploitation libres

Le standard 802.1q est relativement récent et n'est pas encore implémenté nativement dans tous les systèmes d'exploitation, ceux-ci ne pouvant donc interpréter les trames du standard.

Linux

Les noyaux⁴ de version inférieure 2.4.14 doivent être patchés et recompilés afin de pouvoir interpréter les trames taggées. L'utilitaire **vconfig** permet ensuite de configurer les interfaces voulues.

Ex : **vconfig add eth0 1** permet de créer VLAN de VID 5 associé à l'interface eth0.

FreeBSD

La situation est quasi identique à celle de Linux, à l'exception du fait qu'il faut préciser le nombre de vlan que l'on souhaite ajouter à une interface dans le fichier de configuration du noyau avant de le compiler.

Windows

Les version Windows 2000 Server, Windows 2000 Server, Advanced Server et Windows 2000 Datacenter Server supportent plutôt le standard

⁴ <http://www.kernel.org/>

802.1p orientée vers la gestion des priorités. La question reste à examiner pour les releases XP et 2003.

Équipementiers

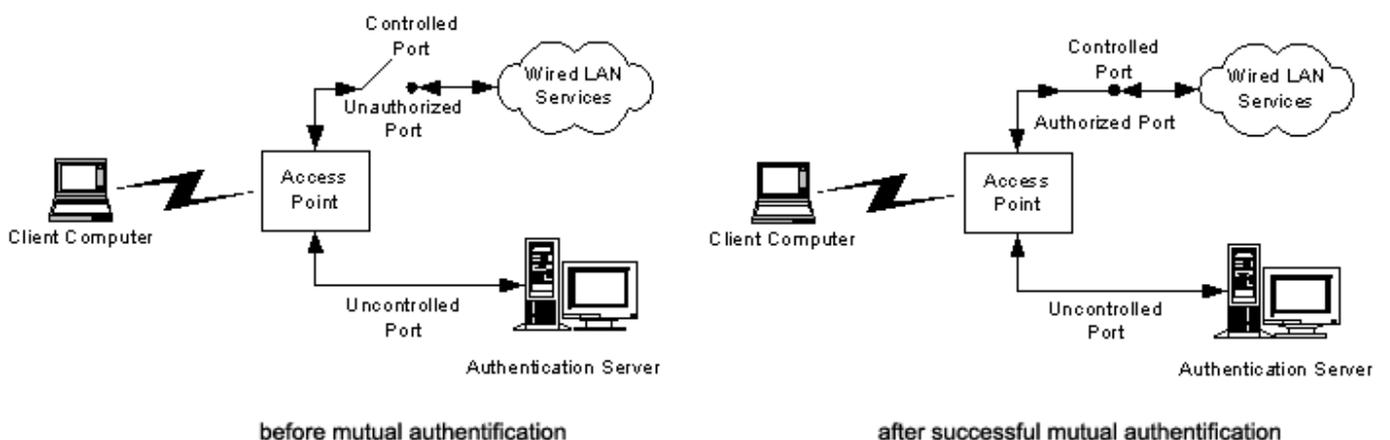
Etant à l'origine de la norme, ils l'implémentent quasiment tous. Les équipementiers les plus importants du marché sont Cisco et 3com. Nous ne décrivons pas les détails d'implémentation qui varient selon les gammes de produits de chaque constructeur et des systèmes d'exploitation propriétaires.

3 Mécanismes d'authentification dans les VLAN

Comme nous allons le voir plus tard, la sécurité des VLAN repose sur les mécanismes mis en œuvre pour l'authentification des machines se connectant aux ports des switches.

Ci-dessous sont détaillées les principales méthodes utilisables pour l'authentification.

- **Fixer une adresse MAC à un port physique** : cette méthode, certes efficace, pose le problème de l'administration qui devient très lourde à gérer notamment lors des déplacements de machines dans le réseau. Ainsi chaque port physique fait partie d'un seul VLAN
- **Port security (propriétaire cisco)** : Cette technologie permet d'implémenter de façon plus souple les règles ci-dessus en indiquant des règles sur les adresses mac permettant de se connecter : une liste de macs autorisés, des conditions de connections (horaires, ...).
- **802.1x (RFC 2284)** Cette norme d'authentification est également employée dans la récente norme de réseaux WIFI 802.11i. On distingue 3 rôles dans le schéma d'authentification :
 - « l'authenticateur » qui met en œuvre l'authentification et route le trafic vers le réseau si l'authentification a marché.
 - le « demandeur » qui demande l'accès au réseau. Dans notre cas, il s'agit de la machine cliente.
 - le « serveur d'authentification » qui effectue l'authentification du demandeur en vérifiant les données qu'il a transmises. La plupart du temps il s'agit d'un serveur radius.



Le concept de « Controlled/Uncontrolled Port »

L'Uncontrolled Port (UP) et le Controlled Port (CP) sont 2 abstractions fonctionnelles qui sont physiquement sur la même connexion réseau. Une trame du client est routée par l'AP (Access Point qui est dans notre cas le switch) vers l'UP ou le CP en fonction de l'état de l'authentification.

Le résultat de cette abstraction logique est que si le client n'est pas authentifié il aura seulement accès au serveur d'authentification. Une fois l'authentification réussie il pourra accéder aux services du réseau.

Un point important est que cette authentification doit être mutuelle ce qui rend quasi impossible toute attaque de type « man in the middle ».

- **Dynamics Vlans (VQP et VMPS)** *propriétaire cisco* : VQP (Vlan Query Protocol) est un protocole qui permet au switch client d'interroger un serveur VMPS (VLAN Membership Policy Server) avec des informations sur les stations enregistrées et leur VLAN associé. Ainsi le switch client pourra associer le port avec le bon VLAN. Le serveur VMPS peut être un switch (ex : cisco catalyst) ou un serveur windows 2000 avec active directory server.

4 La notion de Spanning Tree Protocol

Le spanning tree protocol (STP) permet de manager les connexions Ethernet commutées (exemple par des VLAN). Il fournit des chemins redondants dans un réseau niveau 2 tout en évitant les boucles de routages. Il existe plusieurs types de protocole STP et tous ces types utilisent un algorithme qui calcule le meilleur chemin sans boucle à travers le réseau.

Dans les réseaux Ethernet, un seul chemin actif peut exister entre deux stations. En effet, plusieurs chemins actifs entre des stations causent inévitablement des boucles dans le réseau.

L'algorithme spanning tree fournit des chemins redondants en définissant un arbre qui recense tous les commutateurs dans un réseau étendu et force ensuite certains chemins de données à être à l'état « bloqué ». À intervalles réguliers, les commutateurs dans le réseau émettent et reçoivent des paquets spanning tree qu'ils emploient pour identifier le chemin. Si un segment de réseau devient inaccessible ou si les coûts spanning tree changent, l'algorithme spanning tree reconfigure la topologie spanning tree et rétablit la liaison en activant le chemin de réserve.

Les opérations spanning tree sont transparentes pour les stations d'extrémités, qui ne détectent pas si elles sont connectés à un segment de réseau local simple ou à un réseau local commuté à segments multiples.

5 La notion de trunk, VLAN natif et Dynamic Trunk Protocol

La fonction d'un trunk est de transporter des VLANs entre plusieurs commutateurs interconnectés et donc d'étendre la portée des VLANs à un ensemble de commutateurs. Chaque VLAN est distingué de par ses tags 802.1q ou ICL (protocole CISCO).

Le Dynamic Trunk Protocol (DTP) autorise la configuration automatique de certains ports en mode trunk. Le Switch acceptera donc les traffics taggés et non taggés.

6 La notion de private VLAN (technologie CISCO)

Cette technique permet d'avoir dans un même VLAN des stations qui ne peuvent pas échanger du trafic directement entre elles mais doivent passer par un « port maître ». Cette technique est utilisée, par exemple, pour éviter qu'une station compromise puisse attaquer directement une autre station sur le même VLAN et l'obliger à repasser par le « port maître » ou l'on peut mettre en place un firewall avec une politique de sécurité adéquate.

Cette approche est également très répandue chez les hébergeurs pour des serveurs appartenant à différents clients sur le même VLAN. Il n'y a ainsi pas de communication directe entre les serveurs. Cette solution a l'avantage d'être plus souple que de déclarer un VLAN par client avec des adresse IP, des masques, associé à chaque VLAN.

7 La notion de CDP (Cisco Discovery Protocol)

Ce protocole a été développé par CISCO pour faciliter la découverte d'équipements du réseau et d'échanger des informations exhaustives sur la configuration de ceux-ci :

- Nom et adresse IP de l'équipement
- Version de CatOS/CatIOS/IOS installée
- Plate-forme matérielle et modules installés
- Fonctionnalités de l'équipement
- VLAN natif de l'équipement
- ...

Les messages CDP sont envoyés en multicast.

En dehors de divulguer des informations sur les équipements, ce protocole est très sensible aux denials of services.

En effet les informations échangées par CDP ne sont jamais mises à jour ou remplacées, ainsi il est facile d'envoyer un grand nombre de messages pour saturer la mémoire de l'équipement.

Il est recommandé de désactiver CDP

8 Attaques sur les VLAN

Le point important pour la sécurité d'un VLAN est l'identification du médium de niveau 2 qui permet d'isoler les ports et de faire des traitements en conséquence. Comme on l'a vu, les paquets sont marqués (norme 802.1Q) afin de pouvoir identifier leur provenance et de les traiter en conséquence.

Dans ce panorama les attaques sur l'os des switch VLAN ou la prise de contrôle de la console de management ne sont pas considérées (par brute force par exemple).

Voici la plupart des attaques publiées sur internet jusqu'à ce jour :

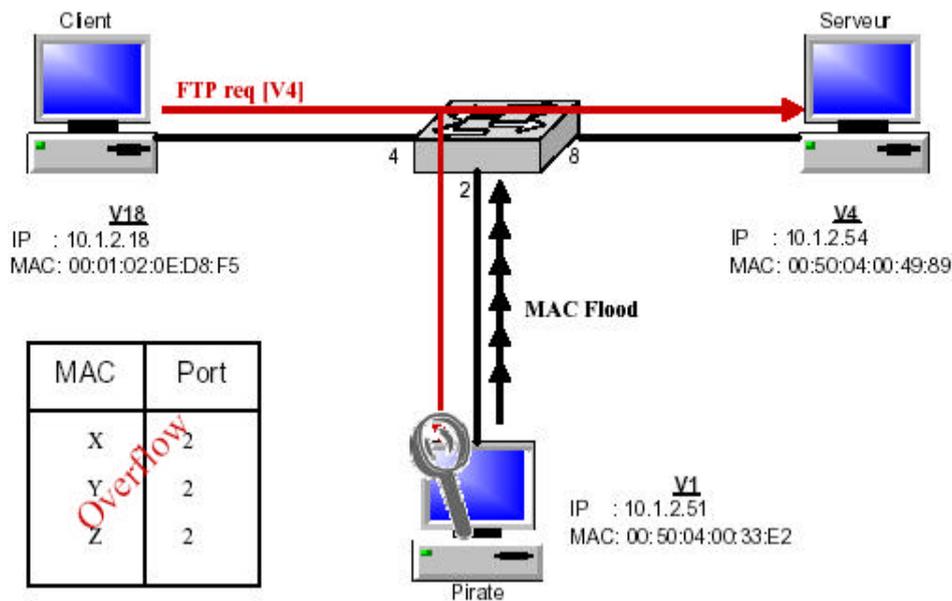
- attaque par MAC Flooding
- attaque par 802.1Q (standard) ISL (CISCO) tagging
- attaque par double encapsulation de 802.1 Q ou nested VLAN
- attaques ARP classiques
- attaques sur les privates VLAN
- attaques par force brute multicast
- attaques sur le spanning tree
- attaques de type random frame stress

8.1 Attaque par MAC Flooding

Description

Cette attaque est basée sur le fait que la table des switch/ponts permettant le « routage » des paquets est limitée.

Schéma de l'attaque :



Dans un premier temps, le pirate va flood le switch avec des arp query/ arp response avec pour chaque demande une adresse MAC différente. Ainsi pour chaque adresse MAC différente, le switch va l'associer dans sa table au port concerné. Le mécanisme est répété jusqu'à saturation de la mémoire : à ce moment le switch ne peut plus enregistrer dans sa table. L'attaque est basée sur le comportement du switch en état de saturation :

- soit il fait un « fail open » : il se transforme en HUB et broadcaste alors toutes les requêtes sur le réseau (le pirate peut alors sniffer toutes les communications).
- Soit il fait un « fail close » : il continue de fonctionner normalement avec sa liste, bien quelle soit pleine et continue de cloisonner efficacement les connexions.

Le comportement du switch saturé est fonction du constructeur. Pour note, les switches « cisco catalyst » continue à cloisonner efficacement les VLAN même lorsqu'ils sont saturés.

Outils pour réaliser l'attaque

Utilitaires pour l'attaque : macof (inclus dans dsniff)

Parades

La parade repose sur l'authentification du connecté afin d'éviter qu'il puisse émettre incognito des trames forgées. Par exemple en activant l'option « port security » sur un switch cisco prenant en paramètre soit une adresse mac ou un nombre maxi d'adresse mac possible. Ainsi le nombre d'association MAC/PORT pour un même port sera limité et les trames incorrectes rejetées.

Ex de commandes pour un switch cisco:

```
CatOS> (enable) set port security mod_num/port_numenable [mac_addr]
CatOS> (enable) set port security mod_num/port_rangeenable maximum [max_mac_addr]
CatOS> (enable) set port security mod_num/port_num mac_addr
CatOS> (enable) show port [mod_num[/port_num]]
```

8.2 Attaques par 802.1Q (standard), ISL (CISCO) tagging

L'idée de cette attaque est de forger des trames permettant d'avoir accès à un autre Vlan en modifiant les tags de la norme 802.1Q.

Une telle attaque repose sur la capacité de forger un tag dans une trame afin de tromper le switch et de sauter de VLAN.

Ex : le switch spoofing :

- L'attaquant envoie des trames forgées avec des tags 802.1Q sur un port quelconque. En principe le switch va rejeter ces trames ou les détagguer étant donné qu'elles ne devraient pas l'être (seul le port du trunk est taggué). Néanmoins, pour les switch cisco par exemple, si le DTP (dynamic trunk protocol) est activé, le port quelconque va se mettre à considérer le port comme un trunk. A partir de la, l'attaquant peut très facilement atteindre tous les VLAN en forgeant une en tête 802.1Q adaptée.

Cette description n'est pas clair. Il vaudrait mieux la reformuler.

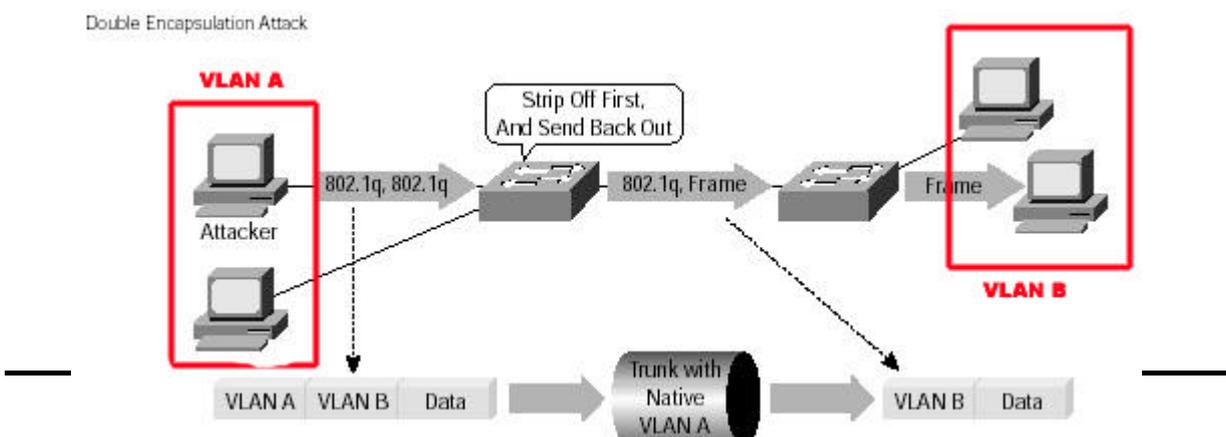
Parade : désactiver absolument le DTP ou tout protocole de détection automatique du port « trunk ».

8.3 Attaque par double encapsulation de 802.1 Q ou nested VLAN

Expliquer ici ce qu'est le vlan natif.

Les trafics de VLAN sont isolés de par les tags 802.1Q (ou ICL pour cisco) rajoutés aux trames Ethernet. La norme 802.1Q introduit des contraintes d'interopérabilité avec les « VLAN natifs » qui n'utilisent pas les tags Ethernet. Ainsi un switch 802.1Q recevant ce type de trame non taggué vont la traiter comme une trame du VLAN natif. Cela permet de dialoguer en « non taggué » avec des anciens switchs non compatibles 802.1Q.

Voici un moyen d'exploiter cette particularité :



Pour que cette attaque réussisse, il est nécessaire que le trunk de transport auquel est relié l'attaquant et la victime soient définis sur le même VLAN natif.

L'attaque consiste à injecter des paquets encapsulés dans 2 trames 802.1q. La trame injectée comporte 2 entêtes 802.1q. La première indiquant le VLAN A et la seconde le VLAN B.

Le switch reçoit cette trame venant d'un VLAN natif avec une entête VLAN A, Il n'est pas normal de recevoir des trames taggées de la part du VLAN A qui est natif : par conséquent le switch enlève le premier tag. En théorie, il devrait se retrouver avec une trame Ethernet sans en tête et dans ce cas la forwarder sur le port physique correspondant au VLAN A. Or lors du traitement de la trame il considère le tag interne VLAN B et à la place dirige la trame vers le VLAN B : le saut de VLAN a été réalisé.

Outil implémentant cette attaque : aucun à notre connaissance

Parade : Cette attaque n'est réalisable qu'à cause d'une mauvaise configuration des switches. Il suffit par exemple d'interdire l'utilisation de VLAN natif pour les utilisateurs, les protocoles STP, CDP continueront à utiliser le VLAN natif. Si l'on ne peut désactiver le VLAN natif, il suffit de désactiver tous les ports avec DTP en mode automatique.

8.4 Attaques ARP classiques

Les attaques ARP classiques sont très largement documentées sur Internet, nous ne reviendrons pas sur leur fonctionnement. Un excellent article concernant le sujet est paru dans MISC 3 et disponible avec des sources l'implémentant à l'adresse <http://www.arp-sk.org/article/arp.html>

Toutes les attaques décrites dans cet article peuvent être mise en œuvre à l'intérieur d'un même VLAN de la même façon que sur un LAN on peut ainsi réaliser une attaque de type man in the middle.

Ce qui nous intéresse ici est une attaque permettant de sauter de VLAN. L'idée est de forger des trames avec une adresse IP source et une adresse MAC source falsifiées et si possible correspondant à une machine sur un autre VLAN.

Selon la façon dont le Switch se comporte, il peut forwarder la trame vers le VLAN souhaité.

Cette attaque n'est valable que pour les Switch qui utilisent des identifications de VLAN basées sur des adresses MAC ou IP.

Outils implémentant ces attaques : outil permettant de forger des trames MAC : arp-sk, dsniiff, taranis.

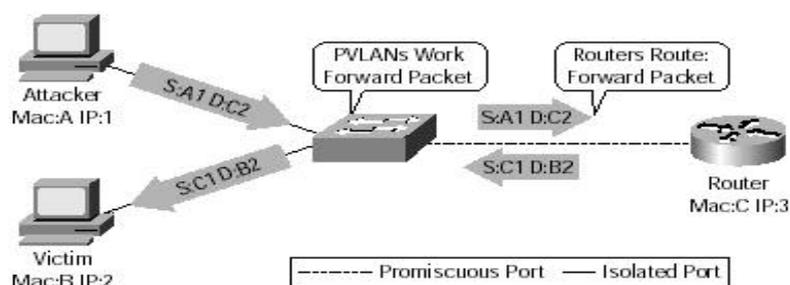
Parades :

Concernant le premier type d'attaque sur le même VLAN : mettre les adresses MAC en statique dans le cache ARP, utiliser des logiciels de surveillance niveau 2 : arpWatch, plugin niveau 2 de prelude, ARP inspection dans les switchs CISCO.

Concernant le saut de VLAN : utiliser une authentification des ports efficace : 802.1q ou 802.1x par exemple.

8.5 Attaques sur les Private LAN

Comme on la vu les Private LAN servent à isoler physiquement les équipements au niveau 2. Néanmoins, il est tout à fait possible de communiquer entre 2 équipements séparés au niveau 2 en passant par le niveau 3, à condition que l'équipement de niveau 3 soit mal configuré.



Dans cet exemple l'attaquant ne peut pas communiquer directement avec la victime mais il lui est possible de l'atteindre en passant par le routeur avec des trames de niveau 3.

Outils implémentant cette attaque : Il ne s'agit pas d'une attaque a proprement dit mais d'une fonctionnalité.

Parade : paramétrage du routeur ou du firewall efficace afin d'empêcher les liens par le niveau 3.

8.6 Attaques par force brute multicast

L'idée est de floodier le switch avec des trames multicast de niveau 2. En principe le switch doit restreindre l'émission de ces trames au VLAN auquel l'émetteur appartient.

Néanmoins, certains switchs peuvent mal se comporter devant la charge et broadcaster sur tous les VLAN pour alléger les traitements. Selon une discussion dans la liste de diffusion bug track. Il semblerait que certains

switchs changent l'algorithme de broadcast et se comportent comme un hub lorsque leur processeur atteint une charge de 70-80% d'utilisation.

Outils implémentant cette attaque : aucun à notre connaissance

Parade : utiliser des switchs non sensibles à cette attaque comme les cisco catalyst.

8.7 Attaques sur le spanning tree

Il y a 2 types d'attaques :

a) **attaque par denials of service** :

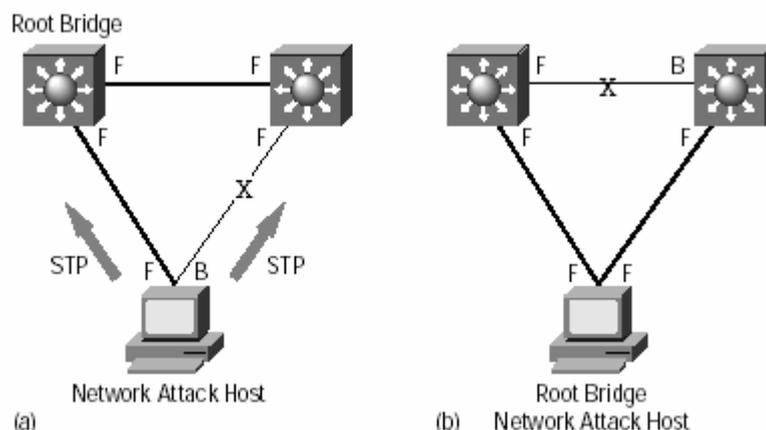
Cette attaque consiste à injecter des BPDU (bridge protocol data unit) falsifiés afin de forcer les équipements à recalculer l'arbre en permanence ce qui rend le réseau inopérant. Il est également possible que sous l'inondation, les switch se transforment en HUB.

Outils implémentant cette attaque : storm

Parade : désactiver STP s'il n'est pas nécessaire, activer le filtrage des BPDU afin d'empêcher l'injection.

b) Par défaut, le protocole STP est activé sur tous les ports. L'attaquant se comporte comme un switch et envoie un BPDU demandant de devenir root (a). L'arbre est recalculé avec comme switch root lui même. Ainsi il peut redéfinir une topologie et intercepter tous le trafic (b):

Pour que cette attaque réussisse de façon transparente, il faut que l'attaquant soit connecté à 2 switchs. Quoi qu'il en soit, l'attaquant peut se faire passer pour un switch et donc intercepter le trafic.



Outils implémentant cette attaque : ethercap (pluggin lamia)
Parade : sous CISCO activer BPDU guard et ROOT guard et désactiver le STP sur les ports ou ne sont pas connectés des switches.

8.8 Random frame Stress Attack

Cette attaque consiste à trouver des failles dans l'implémentation des différents protocoles. Pour cela on fait une attaque exhaustive :

Au niveau de la trame Ethernet :

- On fixe l'adresse mac source et l'adresse mac destination
On essaie toutes les combinaisons possibles sur les autres champs de la trame Ethernet : de la trame : type, bourrage, crc, la taille du paquet, ...
On essaie aussi une multitude de combinaison au niveau arp puisque ce protocole est également pris en compte par le switch pour la mise à jour de ses tables.
- On observe pour voir si un paquet à fait un saut de VLAN ou si le paquet a provoqué une erreur dans le switch par exemple une taille de paquet annoncée différente de la réalité, ... Cette erreur peut être à l'origine d'un buffer overflow.

Outils implémentant cette attaque : aucun connu

Parade : Utiliser un switch avec un OS sûr par exemple les switches cisco catalyst qui ne sont pas sensibles à ces attaques selon les tests faits par @stake.
à ces attaques.

9 Conclusion

Le protocole 802.1Q a pour vocation de spécifier à la fois le comportement des switches et la structure des trames traitées. On constate qu'il doit faire face à plusieurs exceptions dès que l'on se trouve en présence de réseaux hétérogènes tels que Ethenet-FDDI, Ethernet-Token ring, etc. Les vulnérabilités étudiées ont deux origines. Celle sous jacente au protocole hôte dans lequel il faut insérer des tags et celle spécifique au protocole de vlan lui même. L'attaque par MAC flooding est une illustration de la vulnérabilité d'un protocole hôte, permettant de sniffer un vlan par le biais de simples requêtes arp. Pour les attaques reposant sur les tags, dans la plupart des cas il faut arriver à forger des trames avec les entêtes appropriées. Les attaques décrites sont non exhaustives et on peut malheureusement craindre une émergence d'autres types d'attaques. Vu la très grande complexité de la norme, des attaques pourraient être basées sur les bases de données de filtrage, les règles de filtrage et de forwarding et également sur l'intégrité des trames compte tenu de la linéarité du checksum. Enfin pour finir, il est important de noter que suite à cette étude il a été possible de développer les attaques par *broadcast ARP* et par *vlan hopping* en servant de le librairie libnet.1.2. sous Linux Red Hat.

10 Références

Norme IEEE 802.3

Norme IEEE 802.1Q

Norme IEEE 802.2

ISO/IEC 11802-5

<http://www.ieee802.org/1/files/public/docs97/ingress-map.pdf>

Patches de kernel Linux pour support vlan

<http://www.candelatech.com/~greear/vlan.html>

Windows vlan

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/tcpip/part3/tcpch09.asp>

2.rules of vlan operations

http://support.3com.com/infodeli/tools/switches/s_stack2/10012709/10012709/2i3vlaa6.htm

Implémentation linux.

<http://www.candelatech.com/~greear/vlan.html>

A shortcut of tagged and untagged definition of ingress, egress

<http://www.marconi.com/media/vlan100.pdf>

Cisco 802.1q support

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/8021q.htm>

Switching: Trunks and Dynamic Trunking Protocol (DTP)

<http://www.netcraftsmen.net/welcher/papers/switchvtp.html>