Sécurité des ports (switch)

Marvin MANNOY

Ichrak CHERNI

TABLE DES MATIERES :

INTRODUCTION

- La sécurité et les menaces des réseaux sont des sujets importants dans le domaine de la technologie de l'information.

Les réseaux informatiques peuvent être exposés à diverses menaces telles que:

- les logiciels malveillants
- le vol de données
- l'usurpation d'identité
- Ect …

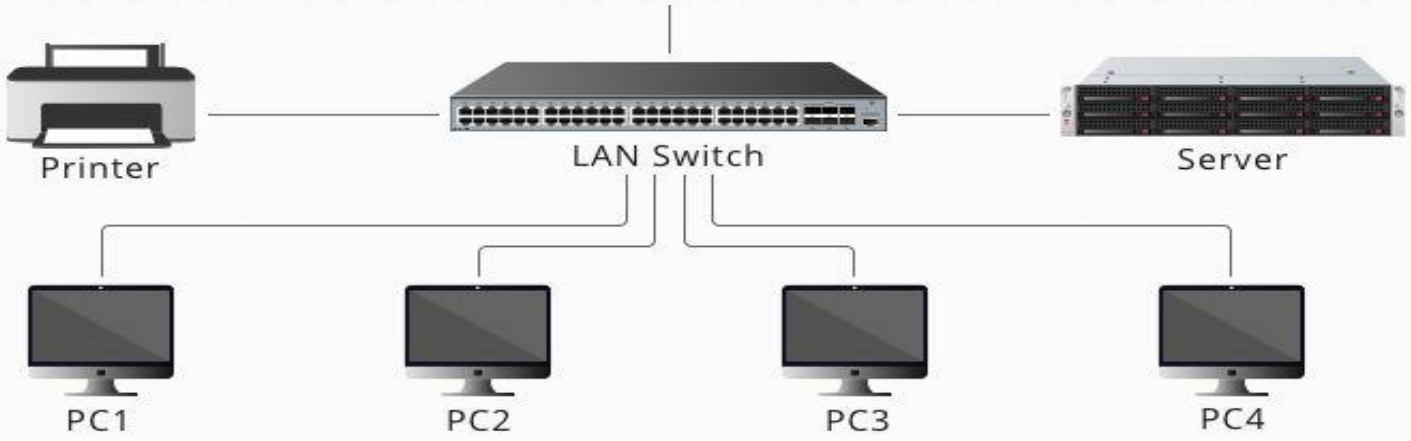
La sécurité des réseaux vise à protéger les fonctionnalités ,l’intégrité de notre réseau et nos données

Sécurité des ports de switch


UN
SWITCH??
UN PORT
DE
SWITCH??
SECURITE
DE PORT DE
SWITCH

- Un switch est un périphérique utilisé dans les réseaux informatiques pour relier plusieurs appareils ensemble. Il agit comme un point central de communication dans un réseau LAN .

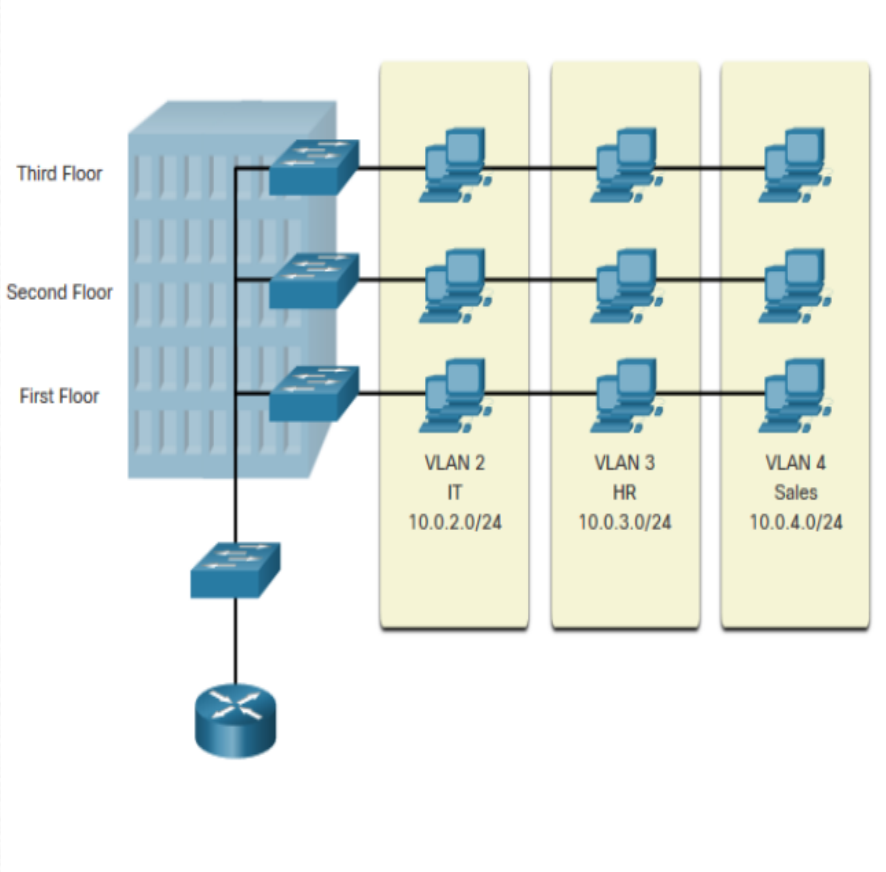
- Un LAN est un réseau informatique qui couvre une zone géographique restreinte, telle qu'une maison, un bureau ou un campus.



- **Un port de switch** est une interface physique qui permet la connectivité entre le switch et les appareils connectés tels que des ordinateurs, des serveurs, des imprimantes, etc. Chaque port de switch peut gérer et acheminer le trafic réseau entrant et sortant.

- En combinant les VLAN avec des fonctionnalités de sécurité telles que la sécurité des ports (DHCP Snooping ,dynamic ARP inspection DAI ,IP source Guard) et les listes de contrôle d'accès (ACLS), les ports de switch peuvent être sécurisés de manière plus robuste.

Les VLANS



Les VLAN (Virtual Local Area Networks) permettent de diviser un réseau en un ou plusieurs sous-réseaux virtuels.

- Chaque VLAN est considéré comme une entité distincte ce qui veut dire que par défaut, ils ne peuvent pas communiquer entre eux.
- Cette solution est moins coûteuse car toute segmentation se fait virtuellement et non physiquement par un appareil.
- Ce cloisonnement permet aussi d'améliorer la vitesse du réseau en diminuant du trafic parasite et en configurant des vitesses précises pour chaque VLAN.

Une fois configuré, chaque VLAN reçoit un tag (balise) lui indiquant son appartenance au VLAN et lui permettant de définir son accès ou non au réseau.

•Le VLAN « poubelle » est utilisé pour rassembler toutes les interfaces physiques (ports) non utilisées du switch dans un VLAN qui n'a pas de connexion avec le réseau.

- ❑ Désactivation des ports : Vous pouvons éteindre les ports non utilisés en les configurant pour être administrativement désactivé. Cela empêchera tout trafic de passer par ces ports et réduira les risques de sécurité liés à des ports inactifs

•Le VLAN natif est utilisé pour déterminer dans quel VLAN les trames non balisées reçues doivent être placées. Il est utilisé pour les appareils qui ne prennent pas en charge le balisage VLAN ou qui envoient des trames sans balisage VLAN.

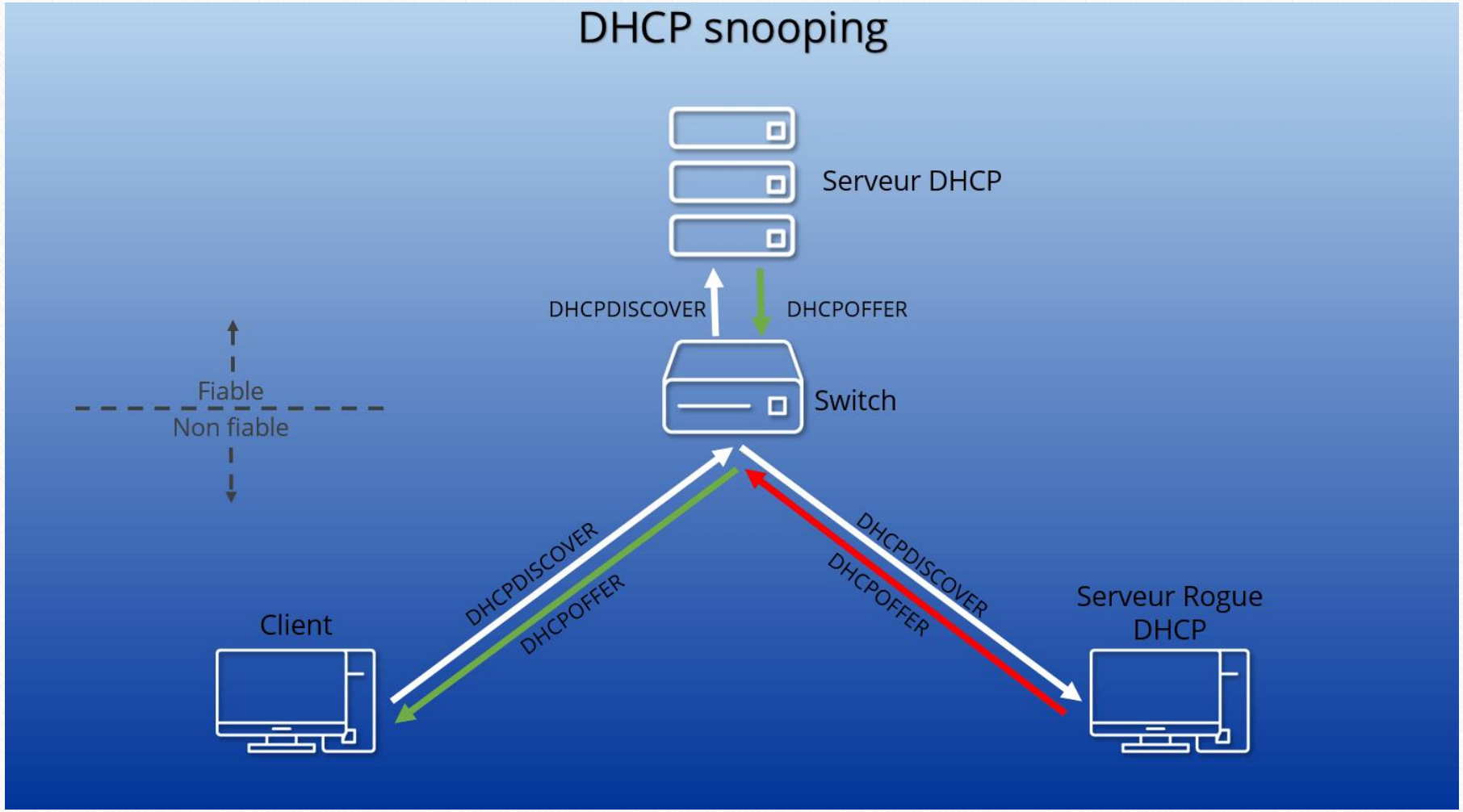
PORT SECURITY

- Port security (sécurité du port) : Nous pouvons configurer le switch pour n'accepter que les adresses MAC préalablement définies, ce qui empêche les appareils non autorisés de se connecter au réseau via ce port.

- La sécurité des ports de switch est principalement axée sur la protection de l'accès physique et la prévention des attaques au niveau du port lui-même.

DHCP snooping

- DHCP snooping : prévient les attaques basées sur le protocole DHCP (Dynamic Host Configuration Protocol) en définissant si un port est fiable ou non.
- Il maintient une table de liaison appelée "binding table" qui associe les adresses IP aux adresses MAC des clients DHCP valides.


DHCP snooping
Serveur DHCP
DHCPDISCOVER
DHCPOFFER
Switch
Fiable
Non fiable
DHCPDISCOVER
DHCPOFFER
DHCPDISCOVER
DHCPOFFER
Client
Serveur Rogue
DHCP

Dynamic ARP Inspection (DAI)

- Dynamic ARP Inspection (DAI) : protège contre les attaques ARP (Address Resolution Protocol) de toutes les interfaces non-fiables en validant si l'adresse MAC de sa table correspond à celle précisée dans l'en-tête du message.

IP Source Guard

- IP Source Guard : bloque tout le trafic provenant des interfaces non-fiable à l'exception des requêtes DHCP, une fois qu'un hôte obtient une adresse IP du DHCP seulement cette adresse IP est permise dans le réseau.

Port-based Authentication (802.1X)

- Port-based Authentication (802.1X) : permet d'authentifier les appareils avant de leur accorder l'accès au réseau, en utilisant des protocoles d'authentification.

LES ACLS

- ACL (Access Control Lists) : Les ACL sont des listes de contrôle d'accès qui permettent de filtrer et de contrôler le flux de trafic réseau sur un switch ou un routeur. Les ACL définissent des règles qui spécifient quel type de trafic est autorisé ou refusé en fonction de critères tels que les adresses IP source et destination, les ports, les protocoles, etc.

Exemple

- Par exemple, nous pouvons créer une règle dans l'ACL pour bloquer le protocole ICMP (Internet Control Message Protocol) afin de prévenir les attaques de type ping ou bloquer le protocole Telnet pour des raisons de sécurité.
- nous pouvons créer une règle dans l'ACL pour autoriser uniquement certaines adresses IP à accéder à un serveur web sur le port 80, tout en bloquant l'accès à partir d'autres adresses IP.

CONCLUSION

- En conclusion, la sécurité des ports de switch vise à contrôler l'accès physique et logique aux ports, en utilisant des mécanismes tels que le port security, le DHCP snooping, le DAI, l'IP Source Guard, l'authentification basée sur le port et les ACLs. Ces mesures de sécurité protègent les ports contre les attaques spécifiques et garantissent l'intégrité du réseau au niveau du port.

MERCI POUR VOTRE ATTENTION