المدرسة العليا للتكنولوجيا- اسفي
ÉCOLE SUPÉRIEURE DE TECHNOLOGIE -SAFI
MARRAKECH
جامعة القاضي عياض
UNIVERSITÉ CADI AYYAD

Département : Informatique
Filière : Génie Informatique
A.U : 2024 / 2025

La mise en œuvre de la sécurité du niveau 2

M 11 : Réseaux Informatiques II

Pr. ESSALIH Mohamed
m.essalih@uca.ac.ma

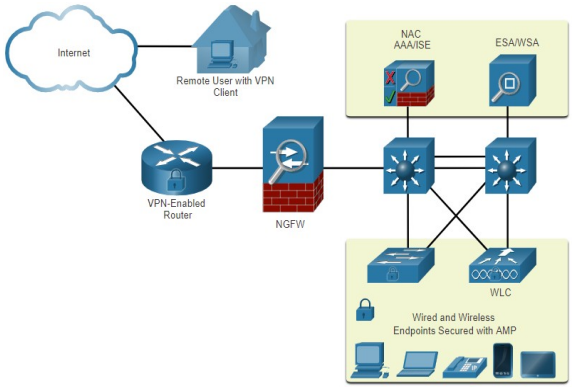
1. Les outils de sécurité des terminaux

Les attaques de réseau & outils de sécurité

- ✓ Les médias d'information couvrent généralement les attaques contre les réseaux d'entreprise.
- ✓ Les attaques réseau peut impliquer :
  1. **Déni de service distribué (DDoS)** - attaque coordonnée de nombreux **zombies** pour dégrader / d'interrompre l'accès du public au site Web & aux ressources d'une organisation.
  2. **Violation de données** - l'attaque où les serveurs de données / hôtes d'une organisation sont compromis pour voler des informations confidentielles.
  3. **Programme malveillant** - l'attaque où les hôtes d'une organisation sont infectés par des logiciels malveillants en provoquant certains problèmes Ex. un **ransomware** (WannaCry, …).
- ✓ Les outils de sécurité d'un réseau pour protéger son périmètre contre tout accès extérieur sont :
  1. **VPN** activé sur un routeur : fournit une connexion sécurisée aux utilisateurs distants.
  2. **Pare-feu** de nouvelle génération (**NGFW**), qui fournit : inspection des paquets avec état - un système de prévention des intrusions de nouvelle génération (**NGIPS**) - protection avancée contre les logiciels malveillants (**AMP**) et un filtrage d'**URL**.
  3. Contrôle d'accès réseau (**NAC**), qui comprend : services d'authentification, d'autorisation et de comptabilité (**AAA**) - **Appliance** de gestion des politiques d'accès sur une grande variété d'utilisateurs et de types d'appareils - moteur de services d'identité de **Cisco** (**ISE**).

Les attaques de réseau & outils de sécurité

- ✓ Les terminaux sont particulièrement sensibles aux attaques liées aux logiciels malveillants, provenant de la messagerie électronique / la navigation **Web**.
- ✓ Les fonctionnalités traditionnelles basées sur l'hôte, utilisées pour les sécurisés sont :
  - ➔ Antivirus / anti-programme malveillant - pare-feu basés sur l'hôte - systèmes de prévention des intrusions (**HIPS**) basés sur l'hôte …
  - ➔ **Cisco ESA :**
    - appareil conçu pour surveiller **SMTP.**
    - constamment mis à jour par des flux en temps réel de **Cisco**
    - **Talos** (détectent et corrèlent les menaces **&** les solutions en utilisant un système de surveillance d'une **BD** mondiale,)
    - **ESA** tire de **TLOS** chaque trois à cinq minutes.
    - bloque les menaces connues – annule les **e-mails** contenant des liens incorrects - chiffrer le contenu des e-mails sortants pour éviter la perte de données - bloquer l'accès aux sites nouvellement infectés.



Les attaques de réseau & outils de sécurité

- **Web Cisco** (**WSA**) :
  - est une technologie d'atténuation des menaces **Web**.
  - aide les organisations à relever les défis de la sécurisation et du contrôle du trafic **Web**.
  - combine une protection avancée contre les logiciels malveillants - la visibilité **&** le contrôle des applications.
  - offre un contrôle complet sur la façon dont les utilisateurs accèdent à Internet.
  - peut **autoriser**, **limiter** avec le temps **&** la bande passante, ou **bloquer**, certaines fonctionnalités **&** applications (Ex. le **chat**, la messagerie, la vidéo et l'audio) selon les besoins de l'organisation.
  - effectue la liste noire / le filtrage / la catégorisation des **URL**,
  - filtre les applications **Web,**
  - analyse les logiciels malveillants,
  - chiffre **&** déchiffre le trafic **Web**.

Le contrôle d'accès

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

- ✓ De nombreux types d'authentification peuvent être effectués sur des périphériques réseau, chacun offre différents niveaux de sécurité.
- ✓ La méthode d'authentification d'accès à distance la plus simple est de configurer une combinaison d'identifiant + mot de passe sur la **console**, les lignes **vty** et les **ports auxiliaires**.
- ✓ **SSH** est une forme d'accès à distance plus sécurisée, qui nécessite (nom d'utilisateur + mot de passe). Qui peuvent être authentifiés localement.
- ✓ La méthode de la base de données locale a certaines limites :
  1. les comptes d'utilisateurs doivent être configurés localement sur chaque périphérique.
  2. elle n'est pas évolutif.
  3. elle ne fournit aucune méthode
  4. d'authentification de secours.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Les outils de sécurité des terminaux

Le contrôle d'accès : AAA

- ✓ Il fournit le cadre principal pour configurer le contrôle d'accès sur un périphérique réseau.
- ✓ Il contrôle **qui est autorisé** à accéder à un réseau (**A**uthentifier) **+** ce qu'il peut faire pendant son accès (**A**utoriser) **+** vérifier les actions effectuées lors de son accès (**C**omptabilité).
- ✓ Les deux méthodes courantes de mise en œuvre de l'authentification **AAA** sont :

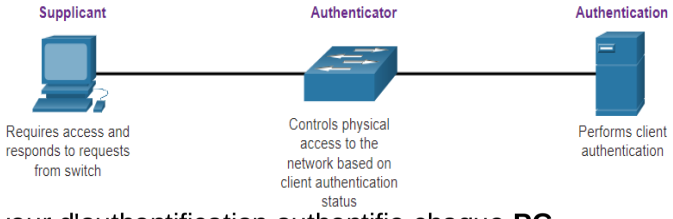
1. **L'authentification AAA locale.**
   - ➢ elle stocke les noms des utilisateurs + les mots de passe localement dans un périphérique réseau (ex. routeur, commutateur, ...).
   - ➢ les authentifications des utilisateurs est à partir de la base de données locale.
   - ➢ elle est idéale pour les réseaux de petite taille.
2. **L'authentification AAA basée sur un serveur :**
   - ➢ les noms d'utilisateur + mot de passe de tous les utilisateurs du réseau sont stockées sur un serveur **AAA** central,
   - ➢ le routeur utilise les protocoles **RADIUS** (Service utilisateur d'accès à distance par authentification) ou **TACACS+** (Contrôleur d'accès aux terminaux Système de contrôle d'accès) pour communiquer avec le serveur **AAA**.
   - ➢ la plus approprié lorsqu'il y a plusieurs routeurs **&** commutateurs.

Les outils de sécurité des terminaux

Le contrôle d'accès : AAA

- ✓ L'autorisation **AAA** :
  - ➢ elle est automatique et ne nécessite aucune étapes supplémentaires à effectuer après l'authentification.
  - ➢ détermine via le serveur **AAA,** ce qu'un utilisateur peut **&** ne peut pas faire sur le réseau (les privilèges **&** les restrictions de l'utilisateur).
- ✓ La comptabilité **AAA** :
  - elle collecte et rapporte les données d'utilisation utilisées pour l'audit ou la facturation,
  - conserve via le serveur **AAA** un journal détaillé de chaque utilisateur authentifié (nom d'utilisateur + la date et l'heure + les commandes saisies par l'utilisateur + heure de début et de fin des connexions + nombre de paquets + le nombre d'octets),
  - le journal est utile lors du dépannage des appareils **&** sert comme preuves lorsque des individus commettent des actes malveillants.

Le contrôle d'accès : la norme IEEE 802.1X



- ✓ C'est un protocole de contrôle d'accès **&**
- ✓ d'authentification basé sur les ports.
- ✓ Il empêche les **PC**s non autorisées de se
- ✓ connecter à un **LAN** via des ports de
- ✓ commutation accessibles au public.
- ✓ Pour accéder aux services du **LAN**, le serveur d'authentification authentifie chaque **PC** connectée à un port de commutation.
- ✓ Les composants de l'authentification **802.1x** sont :

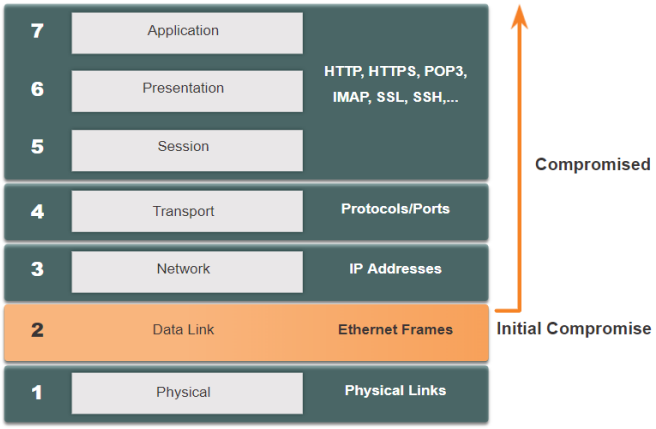
1. **Le client (demandeur)** - appareil exécutant un logiciel client compatible **802.1X**, qui est disponible pour les appareils câblés **ou** sans fil.
2. **L'authentificateur (commutateur / point d'accès sans fil)** - peut servir d'intermédiaire entre le client **&** le serveur d'authentification. 1. Il demande les informations d'identification du client – 2. vérifie ces informations auprès du serveur d'authentification – 3. puis transmet une réponse au client.
3. **Le Serveur d'authentification** – valide l'identité du client + informe L'**authentificateur** que le client est autorisé ou non à accéder au **LAN** et aux services de commutateur.

2. Les menaces de sécurité dans un LAN

Les menaces de sécurité dans un LAN

Les attaques de la couche 2

- ✓ Les solutions de sécurités des couches supérieures (**VPN**, **pare-feu** et **IPS**) sont les plus implémentées régulièrement.
- ✓ L'affectation des couches inférieures, affecte toutes les couches supérieures (Ex. si la trame est capturée => toute la sécurité mise en œuvre ci-dessus serait inutile).
- ✓ La couche 2 est le lien faible du système réseau (à cause de **BYOD** + attaques devenues sophistiquées).



- ✓ Les solutions de sécurité niveau 2 ne seront efficaces que si les protocoles de gestion sont sécurisés.
- ✓ Il faut utiliser :
  - ➔ toujours les variantes sécurisées de protocoles de gestion telles que **SSH**, copie sécurisée (**SCP**), **FTP** sécurisé (**SFTP**) et **SSL** / **TLS** ..
  - ➔ le réseau de gestion hors bande pour gérer les périphériques.
  - ➔ le **VLAN** de gestion dédié où ne réside rien d'autre que le trafic de gestion.
  - ➔ les listes de contrôle d'accès pour filtrer tout accès indésirable.

Les menaces de sécurité dans un LAN

Les attaques de la couche 2

Catégorie	Exemples
1. Les attaques de table MAC	Les attaques par inondation de l'adresse **MAC**.
2. Attaques de VLAN	Les attaques **par saut** + double étiquetage **VLAN**
3. Attaques DHCP	Les attaques d'insuffisance **DHCP** + d'usurpation **DHCP**.
4. Les attaques ARP	Les attaques d'usurpation **ARP** + d'empoisonnement **ARP**.
5. Attaques par usurpation d'adresse	Les attaques d'usurpation d'adresse **MAC** + d'adresse **IP**.
6. Les attaques STP	Les attaques de manipulation du **STP**.

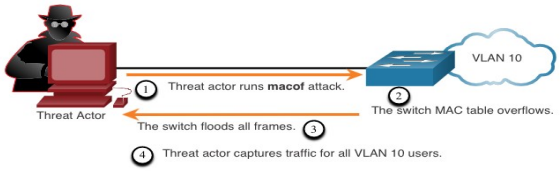
La solution	Description
1. Sécurité des ports	Empêche de nombreux types d'attaques : les attaques d'inondation d'adresses **MAC** + d'insuffisance **DHCP**.
2. Espionnage (snooping) DHCP	Empêche l'insuffisance **DHCP** + attaques d'usurpation du **DHCP**.
3. Inspection ARP dynamique (DAI)	Empêche l'usurpation d'**ARP** + attaques d'empoisonnement d'**ARP**.
4. Protection de la source IP (IPSG)	Empêche les attaques d'usurpation d'adresse **MAC** + **IP**.

Les menaces de sécurité dans un LAN

Les attaques de la table **MAC**

```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

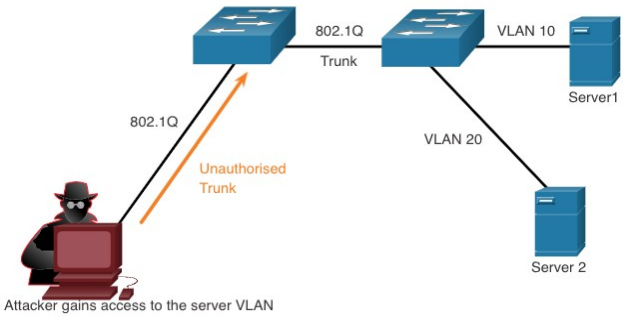
- ✓ La table **CAM** est stockée en mémoire et utilisée pour
- ✓ transmettre plus efficacement les trames.
- ✓ La taille d'une table **MAC** est fixe => un commutateur peut
- ✓ manquer de ressources pour stocker ses adresses **MAC**.
- ✓ Les attaques par inondation (**flooding**) d'adresses **MAC** bombardent le commutateur avec des fausses adresses **MAC** sources jusqu'à ce que sa table soit pleine
- ✓ => le commutateur traite la trame comme une **mono-diffusion** inconnue
- ✓ => Il inonde tout le trafic entrant sur tous les ports du même **VLAN** sans référencer sa table
- ✓ => l'acteur de menace peut capturer toutes les trames échangée sur le **LAN** ou le **VLAN** auquel il est connecté.
- ✓ La table **CAM** peut stocker jusqu'à 132,000 adresses **MAC** => Les attaques d'inondation **CAM** peuvent déborder une table **MAC** très rapidement :
  - L'outil comme **macof** peut inonder un commutateur
  - avec jusqu'à 8,000 faux trames /s
  - ces outils d'attaque affectent tous les
  - commutateurs 2 connectés
  - ces attaques peuvent être atténuées, en
  - implémentant la sécurité des ports (apprendre un nombre limité d'adresses **MAC** sources sur le port.)



Les menaces de sécurité dans un LAN

Les attaques de **LAN** : Attaques de saut de **VLAN**

- ✓ Est l'attaque permettant au trafic d'un **VLAN** d'être détecté par un autre **VLAN** sans l'aide d'un routeur.
- ✓ L'acteur de menace configure un hôte pour qu'il agisse comme un commutateur afin de profiter de la fonction de port de **trunc automatique** activée par défaut sur la plupar des ports de commutateur.



- ✓ L'acteur de menace configure l'hôte pour usurper la **signalisation 802.1Q** et la **signalisation DTP** avec le commutateur de connexion.
- ✓ En cas de succès, le commutateur établit une liaison de **trunc** avec l'hôte
  => l'acteur de menace peut accéder à tous les **VLAN** sur le commutateur
  => Il peut envoyer **&** recevoir du trafic sur n'importe quel **VLAN**, sautant efficacement entre les **VLAN**.

Les menaces de sécurité dans un LAN

Les attaques de **LAN** : Attaque de double étiquetage **VLAN**

- ✓ Est l'attaque où l'acteur de menace incorpore une étiquette **802.1Q** cachée dans la trame, qui a déjà une étiquette **802.1Q.**
- ✓ L'objectif de l'attaque est de gagner l'accès à un **VLAN** que l'étiquette **802.1Q** d'origine n'a pas été spécifié.
- ✓ Les étapes de cette attaque sont :

1. **Étape 1 :** l'acteur de menace envoie une trame **802.1Q** double étiquetage au commutateur. L'en-tête externe a une étiquette **VLAN** de l'acteur de menace, qui est identique au **VLAN natif** du port **trunc**.
2. **Étape 2 :** la trame arrive au premier commutateur, qui examine sa première étiquette **802.1Q** de 4 octets => Le commutateur voit que la trame est destinée au **VLAN natif** => Le commutateur transfère le paquet sur tous les ports **VLAN natif**s après avoir divisé l'étiquette **VLAN**. La trame n'est pas ré-étiquetée car elle fait partie du **VLAN natif**. À ce stade, l'étiquette **VLAN interne** est toujours intacte et n'a pas été inspectée par le premier commutateur.
3. **Étape 3 :** la trame arrive au deuxième commutateur qui ne sait pas qu'elle était destinée au **VLAN natif**. Le deuxième commutateur ne traite que l'étiquetage **802.1Q interne** que l'acteur de menace a insérée en y indiquant que la trame est destinée au **VLAN** cible => Le deuxième commutateur envoie la trame à la cible **ou** l'inonde, selon qu'il existe une entrée de table d'adresses **MAC** existante pour la cible.

Les menaces de sécurité dans un LAN

Les attaques de **LAN** : Attaque de double étiquetage **VLAN**

- ✓ Une attaque de double étiquetage **VLAN** est unidirectionnelle.
- ✓ Elle ne fonctionne que si l'attaquant est connecté à un port résidant dans le même **VLAN** que le **VLAN natif** du port de **trunc**.
- ✓ L'idée est que le double étiquetage permet à l'attaquant d'envoyer des données à des hôtes ou des serveurs sur un **VLAN** qui autrement seraient bloqués par un certain type de configuration de contrôle d'accès (**NAC**).
- ✓ Ces attaques (saut de **VLAN** & double étiquetage **VLAN)** peuvent être évitées / atténuées par :

1. désactivation **trunking** sur tous les ports d'accès.
2. désactivation **trunking** automatique sur les liaisons de **trunc** afin que les **truncs** doivent être activées manuellement.
3. s'assurant que le **VLAN natif** n'est utilisé que pour les liaisons de **trunc**.

Les menaces de sécurité dans un LAN

Les attaques de **LAN** : Attaques de **DHCP**

- ✓ Les deux types d'attaques **DHCP** sont **:**

1. **L'attaque par insuffisance DHCP -** permet de créer un **DoS** en épuisant les ressources **DHCP** via des outils d'attaque tels que **Gobbler** (peut examiner l'intégralité des adresses **IP** louables et les toutes louer en créant des messages de découverte **DHCP** avec de fausses adresses **MAC**).
2. **Attaque d'usurpation DHCP -** elle se produit lorsqu'un serveur **DHCP** non autorisé (**rogue**) se connecte au réseau et fournit la configuration **IP** incorrects aux clients légitimes, telles que :
   - ➢ **Passerelle par défaut incorrecte** - une passerelle invalide **ou** fournit l'adresse **IP** de son hôte (attaque d'homme au milieu).
   - ➢ **Serveur DNS incorrect** - une adresse de serveur **DNS** incorrecte pointant l'utilisateur vers un site **Web** néfaste.
   - ➢ **Adresse IP incorrecte** - une adresse **IP** invalide créant efficacement une attaque **DoS** sur le client **DHCP**.

- ✓ Les deux attaques sont atténuées en mettant en œuvre l'espionnage **DHCP**.

Les menaces de sécurité dans un LAN

Les attaques de **LAN** : Attaques d'**ARP**

- ✓ **ARP** détermine l'adresse **MAC** d'un hôte avec son adresse **IP :**
  1. Tous les hôtes du sous-réseau la reçoivent + la traitent.
  2. L'hôte dont l'adresse **IP** correspond à la requête **ARP** envoie une réponse **ARP**.
- ✓ **ARP gratuite** est la réponse **ARP** non sollicitée envoyé par un client **ARP**

  => Les autres hôtes stockent les adresses **MAC** & **IP** contenues en **ARP gratuite** dans leurs tables **ARP**.
  1. Ex. l'attaquant peut envoyer des réponses **ARP** non sollicitées avec *son adresse **MAC** et l'adresse **IP** de **Gateway*** (attaque d'homme au milieu).
  2. L'attaquant peut envoyer un message **ARP gratuit** avec une adresse **MAC usurpée** à un commutateur/hôte (Le commutateur/hôte mettrait à jour sa table **MAC / ARP**).
- ✓ La découverte de voisin **ICMPv6** est utilisée pour la résolution d'adresse de couche 2 (**IPv6**).
- ✓ **IPv6** comprend des stratégies pour atténuer l'usurpation de publicité de voisin, de la même manière que **IPv4** empêche une réponse **ARP usurpée**.
- ✓ L'**usurpation ARP** & l'**empoisonnement ARP** sont atténués par la mise en œuvre de l'inspection **ARP** dynamique (**DAI**).

Les menaces de sécurité dans un LAN

Les attaques de **LAN** : Attaques par usurpation d'adresse

- ✓ L'usurpation d'adresse **IP** / **MAC** est lorsqu'un acteur de menace détourne une adresse **IP** (**MAC**) valide d'un autre hôte du **LAN /** utilise une adresse **IP** aléatoire.
- ✓ => Il est difficile à l'atténuer, en particulier si elle est utilisée à l'intérieur d'un sous-réseau auquel appartient l'**IP**.
- ✓ Les attaques d'usurpation d'adresse **MAC** :
  - ➢ le commutateur remplace l'entrée de table **MAC** actuelle **&** attribue l'adresse **MAC** au nouveau port.
  - ➢ => Il transfère ensuite par inadvertance des trames destinées à l'hôte cible à l'hôte attaquant.
  - ➢ lorsque l'hôte cible envoie du trafic, le commutateur vérifiera l'erreur, en réalignant l'adresse **MAC** sur le port d'origine.
  - ➢ des **programmes** / **scripts** peuvent être créer pour envoyer constamment des trames au commutateur afin que le commutateur conserve les informations incorrectes ou usurpées.
- ✓ Il n'y a pas de mécanisme de sécurité au couche 2 qui permet à un commutateur de vérifier la source des adresses **MAC**, ce qui le rend très vulnérable à l'usurpation.
- ✓ L'usurpation d'adresse **IP** & **MAC** peut être atténuée en implémentant la protection de la source IP (**IPSG)**.

Les menaces de sécurité dans un LAN

Les attaques de **LAN** : Attaques de **STP**

- ✓ Les attaquants du réseau peuvent manipuler le protocole **STP** pour mener une attaque en usurpant le **pont racine** => *modifiant la topologie d'un réseau*.
- ✓ Les attaquants peuvent alors capturer tout le trafic pour le domaine commuté immédiat.
- ✓ Pour mener une attaque de manipulation **STP**, l'hôte attaquant diffuse des unités de données de protocole de pont **STP** (**BPDU**) contenant de configuration de topologie l'obligera à réévaluer le spanning-tree.
- ✓ Les **BPDU** envoyés par l'hôte attaquant, annoncent une *priorité de pont inférieure* pour tenter d'être élu **pont racine**.
- ✓ Elle peut être atténuée par l'implémentation de **BPDU Guard** sur tous les ports d'accès.

Les attaques de **LAN** : Attaques de la reconnaissance **CDP**

- ✓ Le protocole **CDP** (Cisco Discovery Protocol) est un protocole de découverte de liaison de couche 2. Il est activé par défaut sur tous les périphériques **Cisco**.
- ✓ Il est utilisé aussi pour configurer + dépanner les périphériques réseau. les informations **CDP** sont envoyées sur les ports activés **CDP** dans des diffusions périodiques, non chiffrés et non authentifiées. Les données **CDP** incluent l'adresse **IP** du périphérique, la version logicielle **IOS**, la plate-forme, les fonctionnalités et le **VLAN natif**. Le périphérique qui reçoit le message **CDP** met à jour sa base de données **CDP**.
- ✓ Pour réduire le risque d'attaque de **CDP**, on limite l'utilisation de ce protocole sur les périphériques **&** les ports. Ex. on le désactive sur les ports périphériques qui se connectent aux périphériques non fiables.
- ✓ **no cdp run (cdp run)** du mode de configuration globale est utilisée pour désactiver / activer **CDP** globalement sur un périphérique.
- ✓ **no cdp enable (cdp enable)** du mode de configuration d'interface **est utilisée** pour désactiver / activée **CDP** sur un port.
- ✓ Le protocole **LLDP** (Link Layer Discovery Protocol) est aussi vulnérable aux attaques de reconnaissance. **no lldp run** est utilisée pour désactiver **LLDP** globalement.
- ✓ **no lldp transmite** et **no lldp receive** sur le mode d'interface pour désactiver **LLDP** sur l'interface.

3. La configuration de la sécurité niveau 2

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

- ✓ Les attaques de couche 2 :
  - sont parmi les plus faciles à déployer pour les pirates.
  - Mais elles peuvent également être atténuées facilement.
- ✓ Les solutions de couche 2 courantes possibles sont :
  - tous les ports (interfaces) du commutateur doivent être sécurisés avant que le commutateur ne soit déployé pour une utilisation en production.
  - la façon dont un port est sécurisé dépend de sa fonction.
  - la méthode la plus simple pour protéger le réseau contre les accès non autorisés consiste à désactiver tous les ports inutilisés d'un commutateur.
  - la commande **no shutdown (shutdown)** est utilisée pour désactiver (activer) une interface.
  - **interface range** est utilisée pour configurer une ensemble de ports en même temps :

```
Switch(config)# interface range type module/first-number – last-number
```


La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

- ✓ L'activation de la **sécurité des ports** est la méthode la plus simple **&** la plus efficace pour empêcher les attaques par débordement de la table **CAM.**

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

- ✓ La sécurité des ports :
  - peut être utilisée pour contrôler l'accès non autorisé au réseau,
  - limite le nombre d'adresses **MAC** valides autorisées sur un port,
  - permet à un administrateur de configurer manuellement les adresses **MAC** d'un port,
  - permet au commutateur d'apprendre dynamiquement un nombre limité d'adresses **MAC**,
  - est activée par **switchport port-security** en mode de configuration de l'interface,
  - ne peut être configurée que sur des **ports d'accès** ou de **trunk** de réseau configurés manuellement.
- ✓ A la réception d'une trame, le port configuré avec la sécurité, compare l'adresse **MAC** source du trame à la liste des adresses **MAC** sources sécurisées qui ont été configurées manuellement **ou** apprises dynamiquement sur le port afin de limiter l'accès.
- ✓ A la connexion d'un périphérique au port, le commutateur ajoute automatiquement son adresse **MAC** en tant que **MAC** sécurisé. En dépassant le nombre configuré le port passe **désactivé par erreur**.

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

✓ Pour définir le nombre maximal d'adresses **MAC** autorisées sur un port :

```
Switch(config-if)# switchport port-security maximum value
```

- la valeur de sécurité du port par défaut est 1.
- le nombre maximal des adresses **MAC** sécurisées qui peuvent d'être configurées dépend du commutateur **&** de **IOS**. Ex. le maximum est **8192**.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

✓ Le commutateur peut être configuré pour apprendre les adresses **MAC** sur un port sécurisé :

1. la configuration manuelle d'une / des adresses **MAC** statiques pour chaque port :

```
switchport port-security mac-address mac-address
```

2. apprentissage dynamique **=>** l'adresse **MAC** du nouveau périphérique connecté au port est automatiquement sécurisé **mais** n'est pas ajouté au fichier de configuration en cours.

   => au redémarrage du commutateur, le port devra réapprendre l'adresse **MAC** du périphérique.

3. apprentissage dynamique – Sticky : l'apprentissage est dynamique & ces adresses **MAC** apprises seront «coller» à la configuration en cours :

```
Switch(config-if)# switchport port-security mac-address sticky
```


✓ L'enregistrement en **runing-config** valide l'adresse **MAC** apprise dynamiquement sur **NVRAM**.

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

✓ La sécurité de port complète pour **FastEthernet 0/1** :

- configure manuellement une adresse **MAC** sécurisée - configure le port pour apprendre dynamiquement des adresses **MAC** sécurisées supplémentaires jusqu'à 4 adresses **MAC** sécurisées au maximum.
- **show port-security interface** et **show port-security address** sont utilisées pour vérifier la configuration.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1# show port-security address
            Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports    Remaining Age
                                                                     (mins)
----    -----------       ----                          -----    -------------
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1#
```

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

- ✓ L'obsolescence de la sécurité des ports peut être utilisée pour :
  1. définir le temps d'obsolescence des adresses sécurisées statiques **&** dynamiques sur un port.
  2. supprimer les adresses **MAC** sécurisées sur un port sécurisé sans le faire manuellement.
- ✓ L'obsolescence des adresses sécurisées configurées statiquement peut être activé ou désactivé par port.
- ✓ Pour **activer** / **désactiver** l'obsolescence statique pour le port sécurisé, ou pour définir le temps ou le type d'obsolescence, on utilise :

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
```

```
Switch(config-if)# switchport port-security aging {static | time time | type {absolute | inactivity}
```

- **Absolue** - les adresses sécurisées sur le port sont supprimées après le temps d'obsolescence spécifié (Ex. 10 minutes).
- **Inactivité** - les adresses sécurisées sur le port sont supprimées si elles sont inactives pendant une durée spécifiée.

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

- ✓ La violation de port se produit si l'adresse **MAC** d'un périphérique connecté à un port diffère de la liste des adresses sécurisées => Le port entre dans l'état **désactivé par erreur**.
- ✓ Pour définir le mode de violation de sécurité du port, on utilise :

```
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}
```

Mode	Description
shutdown (par défaut)	Le port passe immédiatement à l'état **désactivé par erreur**, éteint le **LED** du port + envoie un message **Syslog**. Il incrémente le compteur de violations => L'administrateur **doit** le réactiver en entrant les commandes **shutdown** et **no shutdown**
restreindre	Le port supprime les paquets dont l'adresse source est inconnue jusqu'à ce qu'on supprime un nombre suffisant d'adresses **MAC** sécurisées pour passer en dessous de la valeur maximale / augmenter la valeur maximale. Ce mode entraîne l'incrémentation du compteur de violation de sécurité **&** génère un message **syslog**.
protéger	Il s'agit du mode de violation de sécurité le moins sécurisé. Le port supprime les paquets avec des adresses **MAC** source inconnues jusqu'à ce qu'on supprimie un nombre suffisant d'adresses **MAC** sécurisées pour descendre en dessous de la valeur maximale / augmenter la valeur maximale. Aucun message **Syslog** n'est envoyé.

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

- ✓ La violation de sécurité par «**restrict**» est configurée.
- ✓ **show port-security interface** confirme que la modification a été effectuée.
- ✓ Quand un port est fermé et placé dans l'état **error-disabled :**
  - aucun trafic n'est envoyé ou reçu sur ce port
  - une série de messages liés à la sécurité des ports s'affiche sur la console.
  - le protocole de port **+** l'état de la liaison passent à l'état down **&** le voyant du port est éteint.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0050.56be.e4dd:1
Security Violation Count   : 1
S1#
```

```
*Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting Fa0/18 in
err-disable state
*Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address 000c.292b.4c75 on port FastEthernet0/18.
*Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/18, changed state
to down
*Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

- ✓ **show interface** identifie l'état du port comme étant **err-disabled**.
- ✓ **show port-security interface** :
  - ➢ affiche l'état du port comme étant **secure-shutdown**.
  - ➢ le compteur de violation de sécurité incrémente de 1.
  - ➢ l'administrateur doit déterminer la cause de la violation de sécurité.
  - ➢ si un périphérique non autorisé est connecté à un port sécurisé, la menace de sécurité est éliminée avant de réactiver le port.
- ✓ Pour réactiver le port, on utilise d'abord la commande **shutdown** puis on utilise la commande **no shutdown**.

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : c025.5cd7.ef01:1
Security Violation Count   : 1
S1#
```

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

- ✓ Il est recommandé de vérifier que la sécurité des ports est correctement définie.
- ✓ On s'assure que les adresses **MAC** statiques ont été correctement configurées.
- ✓ **Show port-security** affiche les paramètres de sécurité des ports pour le commutateur :
  - Les 24 interfaces sont configurées avec la commande **switchport port-security** car le **maximum autorisé** est 1 et le **mode de violation** est arrêté.
  - Pour chaque interface le **CurrentAddr** (Count) est 0 => Aucun périphérique n'est connecté.
- ✓ **show port-security interface** affiche les détails d'une interface spécifique.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)         (Count)
---------------------------------------------------------------------------
     Fa0/1            1           0                0         Shutdown
     Fa0/2            1           0                0         Shutdown
     Fa0/3            1           0                0         Shutdown
(output omitted)
    Fa0/24            1           0                0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
S1#
```

La configuration de la sécurité niveau 2

Atténuer les attaques de table CAM : La sécurité des ports

- ✓ **show run** permet de vérifier que les adresses **MAC** sont «collées» à la configuration. Ex. **FastEthernet 0/19**.
- ✓ **show port-security address :** affiche toutes les adresses **MAC** sécurisées configurées manuellement / apprises dynamiquement sur toutes les interfaces de commutateur

```
S1# show run | begin interface FastEthernet0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
(output omitted)
S1#
```

```
S1# show port-security address
Secure Mac Address Table
-----------------------------------------------------------
Vlan    Mac Address       Type            Ports     Remaining Age
                                                      (mins)
----    -----------       ----            -----     -------------
1       0025.83e6.4b01    SecureDynamic   Fa0/18          -
1       0025.83e6.4b02    SecureSticky    Fa0/19          -
-----------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

La configuration de la sécurité niveau 2

Atténuer les attaques de VLANs

1. **Étape 1**: On désactive les négociations **DTP** (jonction automatique) sur les ports sans jonction (aucun périphérique) en utilisant **switchport mode access**.
2. **Étape 2**: On désactive les ports inutilisés + On les place dans un **VLAN** inutilisé.
3. **Étape 3**: On active manuellement la liaison de jonction sur un port de jonction en utilisant **switchport mode trunk** .
4. **Étape 4**: On désactive les négociations **DTP** (trunking automatique) sur les ports de jonction en utilisant **switchport nonegotiate**.
5. **Étape 5**: On définit le **VLAN natif** sur un **VLAN** autre que **VLAN 1** en utilisant **switchport trunk native vlan** *vlan_number* .

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```


La configuration de la sécurité niveau 2

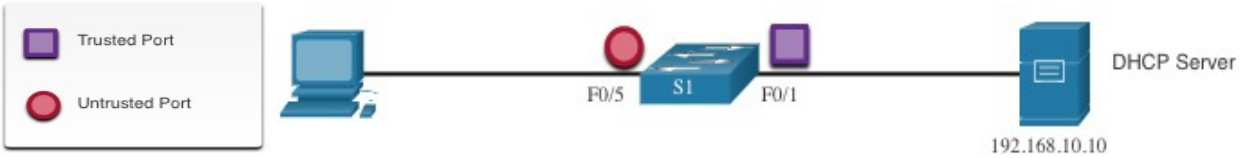
Atténuer les attaques DHCP : Surveillance du DHCP

- ✓ L'**attaque de famine DHCP** utilise un outil d'attaque (Ex.**Gobbler)** pour créer un déni de service (**DoS**). Pour connecter les clients **Gobbler** :
  - ➔ utilise une adresse **MAC** source unique pour chaque demande **DHCP** envoyée => Ce type d'attaque peut être efficacement atténuées en utilisant la sécurité des ports.
  - ➔ peut être configuré pour utiliser l'adresse **MAC** de l'interface réelle comme adresse **Ethernet** source, mais spécifie une adresse Ethernet différente dans la charge utile **DHCP** => la sécurité du port inefficace car l'adresse **MAC** source serait légitime.
- ✓ La **surveillance DHCP** filtre les messages **DHCP** en limitant le trafic **DHCP** sur les ports non approuvés :
  - ➢ les périphériques sous contrôle administratif (commutateurs, routeurs et serveurs) sont des sources fiables. ⇒ leurs interfaces doivent être explicitement configurées comme sécurisées.
  - ➢ les périphériques en dehors du réseau **&** tous les ports d'accès sont généralement traités comme des sources non fiables.
- ✓ **Table d'espionnage DHCP** : est une table crée en liant l'adresse **MAC** source d'un périphérique sur *un port non approuvé* **&** son adresse **IP** attribuée par le serveur **DHCP**.

La configuration de la sécurité niveau 2

Atténuer les attaques DHCP : Surveillance du DHCP

1. **Étape** 1. **ip dhcp snooping** est utilisée pour activer la surveillance **DHCP** en mode de configuration globale.
2. **Étape 2**. sur les ports approuvés, on utilise **ip dhcp snooping trust** en mode de configuration de l'interface.
3. **Étape 3**: sur les interfaces non fiables, limitation du nombre de messages de découverte **DHCP** pouvant être reçus en utilisant **ip dhcp snooping limit rate** *packets-per-second* en mode de configuration d'interface.
4. **Étape 4**. activation de la surveillance **DHCP** par **VLAN**, ou par une **portée de VLAN**, en utilisant **ip dhcp snooping** *vlan* en mode de configuration globale.



- La surveillance **DHCP** est d'abord activé sur **S1**.
- L'interface en amont du serveur **DHCP** est explicitement approuvée.
- **F0 / 5** à **F0 / 24** ne sont pas approuvés et sont donc limités à six paquets par seconde.
- La surveillance **DHCP** est activée sur les **VLANS 5, 10, 50, 51** et **52**.

La configuration de la sécurité niveau 2

Atténuer les attaques DHCP : Surveillance du DHCP

- ✓ **show ip dhcp snooping** permet de vérifier les paramètres de **snooping DHCP**.
- ✓ **show ip dhcp snooping binding** permet d'afficher les clients qui ont reçu des informations **DHCP**.
- ✓ **N.B**: **Snooping DHCP** est également requis par l'**inspection ARP** dynamique (**DAI**).

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                  Trusted    Allow option    Rate limit (pps)
-------------------------  -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5            no         no              6
  Custom circuit-ids:
FastEthernet0/6            no         no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:03:47:B5:9F:AD   192.168.10.10    193185      dhcp-snooping  5     FastEthernet0/5
```

La configuration de la sécurité niveau 2

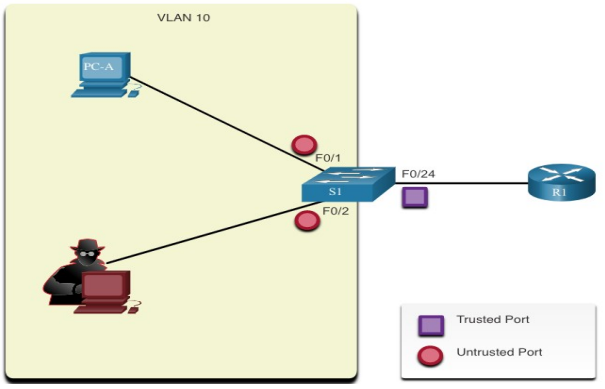
Atténuer les attaques ARP : Inspection **ARP** dynamique

- ✓ Pour empêcher l'**usurpation ARP** & l'**empoisonnement ARP**, le commutateur **doit** garantir que seules les demandes **&** réponses **ARP** *valides* sont relayées.
- ✓ L'**I**nspection **ARP** **D**ynamique (**DAI**) nécessite la **snooping DHCP**, pour :
  1. intercepter toutes les demandes **&** réponses **ARP** sur des ports **non approuvés**.
  2. vérifier chaque paquet intercepté pour une liaison **IP - MAC** valide.
  3. ne relayer pas les réponses **ARP non valides** / **gratuites** vers d'autres ports du même **VLAN**.
  4. abandonner **&** journaliser toutes les réponses **ARP** provenant de ports non valides pour empêcher l'**empoisonnement ARP**.
  5. **Erreur-désactivation** de l'interface si le nombre **DAI** de paquets **ARP** configuré est dépassé.
- ✓ Pour activer le **DAI** :
  1. activation globale de **snooping DHCP**.
  2. activation de **snooping DHCP** sur les **VLAN** sélectionnés.
  3. activation de **DAI** sur les **VLAN** sélectionnés.
  4. configuration des interfaces sécurisées pour la **snooping DHCP** et l'**inspection ARP**.

La configuration de la sécurité niveau 2

Atténuer les attaques ARP : Inspection **ARP** dynamique

- ✓ Il est généralement conseillé de configurer :
  1. tous les ports de commutateur d'**accès** comme **non approuvés**
  2. tous les ports de liaison montante **connectés à d'autres commutateurs** comme **approuvés**.
- ✓ Dans la topologie, **S1** connecte deux utilisateurs sur le **VLAN 10**.
- ✓ **DAI** a été configuré pour atténuer les attaques d'**usurpation ARP** & d'**empoisonnement ARP** :
  - ➔ **Snooping DHCP** est activée car **DAI** nécessite sa table de liaison pour fonctionner.
  - ➔ **snooping DHCP** et l'**inspection ARP** sont activés pour les **PC** sur **VLAN10**.
  - ➔ le port de liaison montante vers le routeur est approuvé => configuré comme **approuvé** pour **snooping DHCP** et l'**inspection ARP**.




```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

La configuration de la sécurité niveau 2

Atténuer les attaques ARP : Inspection **ARP** dynamique

- ✓ **DAI** peut également être configuré pour vérifier l'adresse :
  - ➢ **MAC de destination** sur l'en-tête **Ethernet** par rapport à l'adresse **MAC** cible dans le corps **ARP**.
  - ➢ **MAC de source** sur l'en-tête **Ethernet** par rapport à l'adresse **MAC** de l'expéditeur sur le corps **ARP**.
  - ➢ **IP** du corps **ARP** pour les adresses **IP invalides** et **inattendues**, y compris les adresses **0.0.0.0**, **255.255.255.255** et toutes les adresses de **multi-diffusion IP**.
- ✓ **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} (configuration globale) configure **DAI,** pour supprimer les paquets **ARP** lorsque :
  - ➔ les adresses **IP** ne sont pas valides.
  - ➔ les adresses **MAC** des paquets **ARP** ne correspondent pas aux adresses spécifiées dans l'**en-tête Ethernet**.

La configuration de la sécurité niveau 2

Atténuer les attaques ARP : Inspection **ARP** dynamique

- ➢ **N.B :** La saisie de plusieurs commandes **ip arp inspection validate** écrase la commande précédente.
- ➢ => Pour inclure plusieurs méthodes de validation, on saisit sur la même ligne de commande.

```
S1(config)# ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```


La configuration de la sécurité niveau 2

Atténuer les attaques **STP** : **PortFast** et **BPDU Guard**

- ✓ Pour atténuer les attaques **STP**, on utilise :
  1. **PortFast** :
     - il amène immédiatement un port à l'**état de transfert** à partir d'un **état de blocage**.
     - s'applique à tous les **ports d'accès** d'utilisateur final.
     - **PortFast** sur les liaisons inter-commutateurs peut créer une boucle de **STP**.
  2. Protection **BPDU Guard** :
     - il désactive immédiatement « **par erreur »** un port qui reçoit une unité **BPDU**.
     - elle ne doit être configurée que sur les interfaces connectées aux périphériques d'extrémité.

La configuration de la sécurité niveau 2

Atténuer les attaques **STP** : Configuration de **PortFast**

- ✓ **spanning-tree portfast** de configuration d'interface est utilisée pour activer **PortFast** sur une interface.
- ✓ **spanning-tree portfast default** de configuration globale est utilisée pour activer **PortFast** sur tous les ports d'accès.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
```

- ✓ Pour vérifier si **PortFast** est activé globalement, on peut utiliser soit :
  1. **show running-config | begin span**
  2. **show spanning-tree summary**
- ✓ Pour vérifier si **PortFast** est activé sur une interface, on peut utiliser
  1. **show running-config interface** *type/number*
  2. **spanning-tree interface** *type/number* **detail**

Atténuer les attaques **STP** : **BPDU Guard**

- ✓ Un **port d'accès** pourrait recevoir des **BPDU inattendus** accidentellement / lorsqu'un utilisateur connecte un commutateur **non autorisé** au **port d'accès**.
- ✓ Si une **BPDU** est reçue sur un port d'**accès activé** par **BPDU Guard**, le port est mis en état désactivé par erreur.
- ✓ **spanning-tree bpduguard enable** de configuration d'interface est utilisée pour activer **BPDU Guard** sur une interface

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

- ✓ **spanning-tree portfast bpduguard default** de configuration globale est utilisée pour activer **BPDU Guard** globalement sur tous les **ports d'accès**.

Questions & Discussion