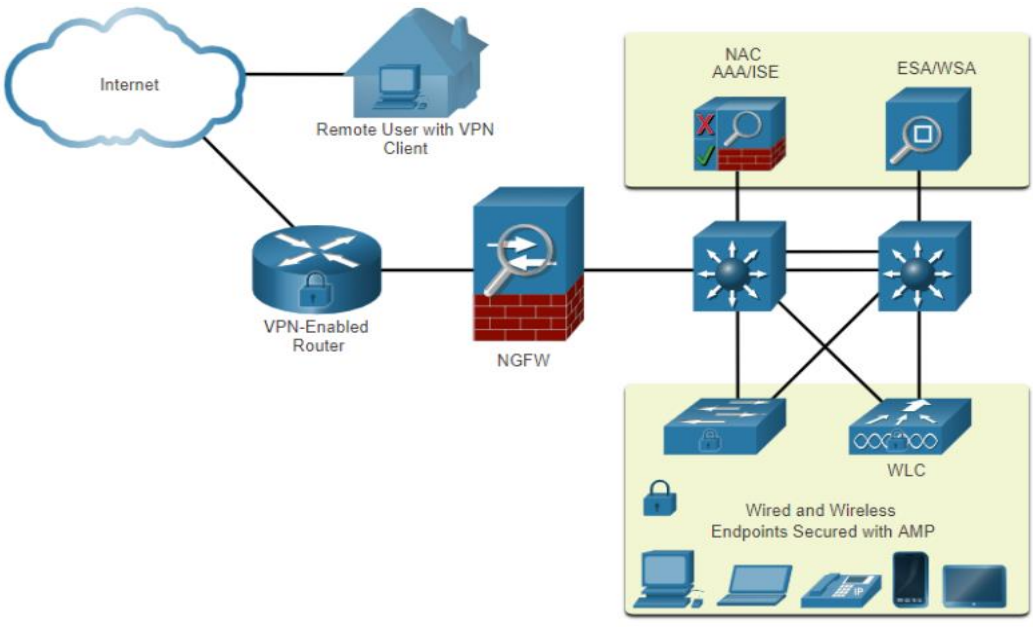
Chapitre 08	Sécuriser un réseau LAN

1. Concepts de sécurité LAN

1.1. Protection des terminaux

- Les terminaux réseaux (ordinateur, serveur, imprimante, …) sont toujours menacés par des attaques informatiques telles que :
  - **Déni de service distribué (DDoS)**
  - **Violation de données confidentielles**
  - **Logiciel malveillant (virus, malware, ...)**
- Les terminaux sont particulièrement sensibles aux attaques liées **aux logiciels malveillants** qui proviennent de la messagerie électronique, de la navigation Web, d'une clé USB, etc.
- Ces terminaux utilisent généralement des fonctionnalités de **sécurité traditionnelles** basées sur l'hôte (antivirus/antispyware, pare-feu lié au système d'exploitation, HIDS/HIPS, …) et peuvent aussi être mieux protégés par divers appareils de sécurité du réseau comme :
  - **Routeur activé VPN** qui fournit une connexion sécurisée aux utilisateurs distants sur un réseau public et sur le réseau d'entreprise.
  - **Pare-feu de nouvelle génération (NGFW)** qui fournit une inspection des paquets avec état, un contrôle des applications, une protection avancée contre les logiciels malveillants (AMP), etc.
  - **Contrôle d'accès réseau (NAC)** qui comprend les services d'authentification, d'autorisation et de comptabilité (AAA).



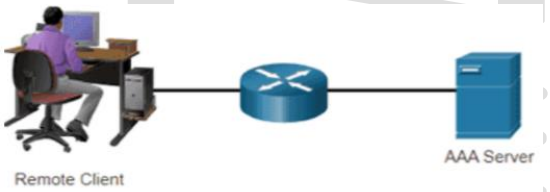
1.2. Authentification avec mot de passe local

- De nombreux types d'authentification peuvent être effectués sur des périphériques réseau, et chaque méthode offre différents niveaux de sécurité.
- La méthode d'authentification d'accès à distance la plus simple et la plus sécurisée est d'utiliser **SSH**.
- Voici un rappel sur les commandes de configuration de SSH sur un routeur R1 :

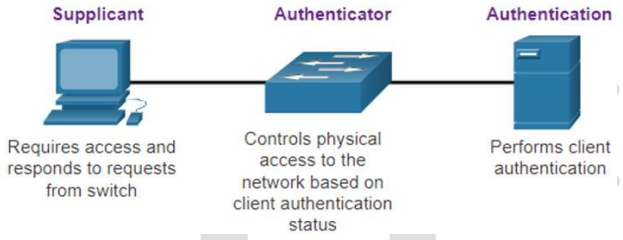
```
R1(config)# ip domain-name ofppt.ma
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

1.3. AAA et 802.11x

- **AAA** signifie **A**uthentication (authentification), **A**uthorization (autorisation) et **A**ccounting (traçabilité).
- AAA est un moyen de contrôler qui est autorisé à accéder à un réseau (authentifier), ce qu'ils peuvent faire pendant leur séjour (autoriser), et d'auditer les actions qu'ils ont effectuées lors de l'accès au réseau (comptabilité).



- La norme **IEEE 802.1x** est un protocole de contrôle d'accès et d'authentification basé sur les ports.
- Le protocole 802.1x empêche les stations de travail non autorisées de se connecter à un réseau local via des ports de commutation accessibles au public.
- Avec une authentification 802.1x basée sur les ports, les périphériques réseau ont des rôles spécifiques :
  - Le client (demandeur)
  - Le commutateur (authentificateur)
  - Le Serveur d'authentification



1.4. Catégories des attaques sur les commutateurs

- Voici les types d'attaques réseau liées au commutateur :

Attaques de la table MAC	Il comprend les attaques par inondation de l'adresse MAC.
Attaque de VLAN	Il comprend les attaques par saut et par revérifier VLAN
Attaques DHCP	Attaques d'insuffisance DHCP et d'usurpation DHCP
Attaques ARP	Attaques d'usurpation ARP et d'empoisonnement ARP
Attaques par usurpation d'adresse	Attaques d'usurpation des adresses MAC et IP
Attaque STP	Attaques de manipulation du protocole Spanning-tree.

- Plusieurs solutions permettent d'atténuer les attaques du commutateur :

Sécurité des ports	Empêche les attaques d'inondation d'adresse MAC et d'insuffisance DHCP.
Espionnage DHCP	Empêche l'insuffisance DHCP et les attaques d'usurpation de DHCP.
Inspection ARP dynamique (DAI)	Empêche les attaques d'usurpation ARP et d'empoisonnement ARP.
Protection de la source IP (IPSG)	Empêche les attaques d'usurpation d'adresse MAC et IP.

2. Sécurité des ports du commutateur

2.1. Désactiver les ports non utilisés

- Désactiver les ports du commutateur non utilisés est une méthode simple mais efficace à laquelle les administrateurs ont recours pour mieux protéger le réseau contre tout accès non autorisé.
- La désactivation des ports du commutateur se fait par la commande **shutdown**.
- Il est possible de désactiver une plage de ports sur un commutateur via la commande **interface range**.

2.2. Implémenter la sécurité des ports

- Tous les ports de commutateur doivent être sécurisés avant le déploiement du commutateur en production.
- L'une des méthodes de sécurisation des ports consiste à implémenter une fonctionnalité appelée **sécurité des ports**.
- La sécurité des ports restreint le nombre d'adresses MAC autorisées sur un port.
- Il existe trois types d'adresses MAC sécurisées :

Adresses MAC sécurisées statiques	Adresses MAC configurées **manuellement** sur un port avec la commande **switchport port-security mac-address *adresse-mac*.** Elles sont stockées dans la table d'adresses MAC et sont ajoutées à la configuration en cours sur le commutateur (fichier running-config).
Adresses MAC sécurisées dynamiques	Adresses MAC apprises de manière dynamique. Elles sont stockées uniquement dans la table d'@MAC et supprimées au redémarrage du commutateur.
Adresses MAC sécurisées rémanentes	Adresses MAC pouvant être apprises de manière dynamique ou configurées manuellement. Elles sont stockées dans la table d'@MAC et ajoutées à la configuration en cours.

- Il y a violation de la sécurité lorsque l'une des situations suivantes se présente :
  - Le nombre maximal d'adresses MAC sécurisées a été ajouté dans la table d'adresses de l'interface et une station dont l'adresse MAC ne figure pas dans la table d'adresses tente d'accéder à l'interface.
  - Une adresse assimilée ou configurée dans une interface sécurisée est visible sur une autre interface sécurisée dans le même VLAN.

- Une interface peut être configurée pour l'un des **trois modes de violation**, en spécifiant les actions à entreprendre en cas de violation :

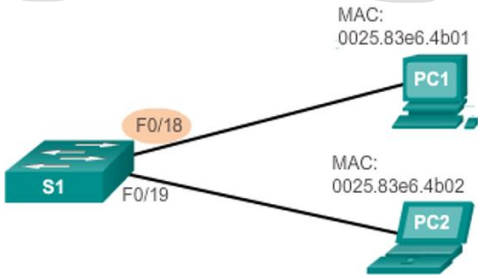
Mode de violation	Acheminement du trafic	Envoi d'un message syslog	Arrêt du port
Protect	Non	Non	Non
Restrict	Non	Oui	Non
Shutdown	Non	Oui	Oui

- Voici les paramètres par défaut de la sécurité des ports sur les commutateurs Cisco :

Sécurité des ports	Désactivée sur un port
Nombre maximal d'adresses MAC sécurisées	1
Mode de violation	Shutdown. Le port est désactivé en cas de dépassement du nombre maximal d'adresses MAC sécurisée.
Apprentissage des adresses rémanentes	Désactivé

- Exemple : configuration de la sécurité des ports dynamiques

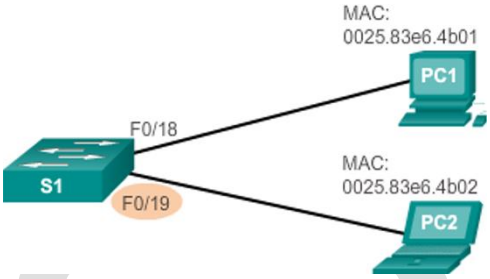
Spécifier le port à configurer	S1(config)# **interface Fa0/18**
Définir le port en mode d'accès	S1(config-if)# **switchport mode access**
Activer la sécurité des ports	S1(config-if)# **switchport port-security**



Show mac address-table

- Exemple : configuration de la sécurité des ports rémanents

Spécifier le port à configurer	S1(config)# **interface Fa0/19**
Définir le port en mode d'accès	S1(config-if)# **switchport mode access**
Activer la sécurité des ports sur le port	S1(config-if)# **switchport port-security**
Définir le nombre maximal d'adresses sécurisées autorisées sur le port	S1(config-if)# **switchport port-security maximum 50**
Activer l'apprentissage rémanent	S1(config-if)# **switchport port-security mac-address sticky**



- Voici les commandes de vérification des adresses MAC sécurisées :
  - **Show running-config**
  - **Show port-security interface fa0/18**
  - **Show port-security address**