Étude comparative 802.1X et Port-Security

Thomas CISERANE

8 janvier 2025

Table des matières

Résumé

La sécurisation des réseaux locaux constitue une priorité dans la protection des ressources internes et la prévention des accès non autorisés. Ce document explore deux mécanismes complémentaires : Port Security, une méthode de contrôle basée sur les adresses MAC, et IEEE 802.1X, une solution avancée d'authentification au niveau du port utilisant un serveur RADIUS. Après une présentation de leur fonctionnement, leurs avantages et leurs limites respectives, une analyse comparative met en évidence leur complémentarité dans différents scénarios.

1 Introduction

La sécurité des réseaux locaux est un enjeu crucial pour prévenir les accès non autorisés et garantir la protection des ressources internes. Avec la multiplication des dispositifs connectés et l'évolution constante des menaces, il est essentiel de mettre en place des mécanismes robustes pour contrôler l'accès au réseau.

Deux mécanismes de sécurité couramment utilisés dans ce cadre sont :

— **Port Security** : une méthode simple et efficace pour limiter les accès à un commutateur en se basant sur les adresses MAC. Elle permet de restreindre le nombre de périphériques pouvant se connecter à un port donné et de définir des actions en cas de détection d'adresses MAC non autorisées.

— **IEEE 802.1X** : une solution plus avancée basée sur l'authentification au niveau du port, souvent associée à des serveurs RADIUS. Ce protocole offre une authentification dynamique des dispositifs avant leur accès au réseau, renforçant ainsi la sécurité en s'assurant que seuls les utilisateurs et appareils autorisés peuvent se connecter.

Dans le cadre de ce rapport, nous chercherons à comparer ces deux approches en termes de fonctionnalités, cas d'utilisation et efficacité, tout en explorant leur complémentarité potentielle. Nous analyserons comment ces mécanismes peuvent être déployés pour renforcer la sécurité des réseaux locaux et quelles sont les meilleures pratiques pour leur mise en œuvre.

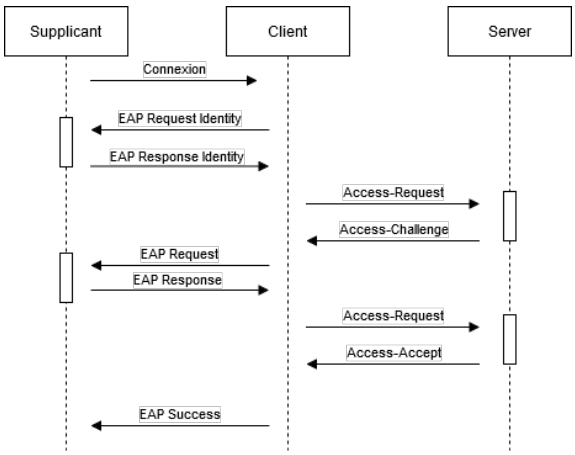

FIGURE 1 – Schéma de connexion à un réseau

2 Présentation des technologies

Le protocole **IEEE 802.1X** est une norme d'authentification au niveau des ports réseau, conçue pour contrôler l'accès aux réseaux filaires et sans fil. Il assure que seuls les utilisateurs et dispositifs autorisés peuvent se connecter, renforçant ainsi la sécurité du réseau.

2.1 IEEE 802.1X

2.1.1 Fonctionnement général

Le processus d'authentification 802.1X implique trois acteurs principaux :

— **Supplicant (Demandeur)** : le dispositif client qui souhaite accéder au réseau.

— **Authenticator (Authentificateur)** : généralement un commutateur ou un point d'accès qui contrôle l'accès au réseau.

— **Authentication Server (Serveur d'authentification)** : souvent un serveur AAA utilisant le protocole RADIUS, responsable de valider les informations d'identification du supplicant.

Le processus d'authentification suit généralement ces étapes :

1. **Initiation** : Le supplicant se connecte à un port contrôlé par l'authenticator.
2. **Déclenchement** : L'authenticator détecte la connexion et initie une demande d'authentification.
3. **Échange EAP** : Le supplicant et l'authenticator échangent des messages EAP pour transmettre les informations d'identification au serveur d'authentification.
4. **Validation** : Le serveur d'authentification vérifie les informations reçues.
5. **Autorisation** : Si l'authentification est réussie, le serveur informe l'authenticator, qui ouvre le port pour permettre l'accès au réseau.
6. **Supervision** : L'authenticator continue de surveiller le port pour détecter toute activité suspecte ou déconnexion.

2.1.2 Rôle du protocole EAP

Le **Extensible Authentication Protocol (EAP)** est un cadre utilisé pour transporter les informations d'authentification entre le supplicant, l'authenticator et le serveur d'authentification. EAP prend en charge divers mécanismes d'authentification, tels que les certificats numériques, les identifiants utilisateur/mot de passe, et les cartes à puce, offrant ainsi une flexibilité dans le choix des méthodes d'authentification adaptées aux besoins spécifiques du réseau.

2.1.3 Serveur AAA et protocole RADIUS

Dans le cadre de 802.1X, le serveur d'authentification est souvent un serveur **AAA** qui gère les trois fonctions clés :

— **Authentication (Authentification**) : Vérification de l'identité du supplicant.

— **Authorization (Autorisation)** : Détermination des ressources réseau auxquelles le supplicant peut accéder.
— **Accounting (Comptabilité)** : Suivi et enregistrement des activités du supplicant sur le réseau.

Le protocole **Remote Authentication Dial-In User Service (RADIUS)** est couramment utilisé pour communiquer entre l'authenticator et le serveur AAA. RADIUS transporte les informations d'authentification et d'autorisation, et peut également être utilisé pour appliquer des politiques spécifiques, comme l'affectation dynamique de VLANs ou l'application de listes de contrôle d'accès (ACL).

2.1.4 Avantages de l'utilisation de 802.1X

— **Sécurité renforcée** : En exigeant une authentification avant l'accès au réseau, 802.1X empêche les dispositifs non autorisés de se connecter.
— **Contrôle d'accès granulaire** : Permet l'application de politiques spécifiques par utilisateur ou par dispositif.
— **Intégration avec des annuaires existants** : Peut être intégré avec des services d'annuaire tels qu'Active Directory pour une gestion centralisée des identités.
— **Flexibilité des méthodes d'authentification** : Prend en charge diverses méthodes d'authentification via EAP, adaptées aux besoins spécifiques de l'organisation.

2.2 Port Security

Le Port Security (Port Security) est une fonctionnalité des commutateurs Cisco conçue pour sécuriser un port d'accès (connecté à une station de travail, un serveur, etc.) en surveillant les adresses MAC source des trames Ethernet reçues sur ce port. En cas de violation, une action est automatiquement déclenchée.
Cette fonctionnalité peut être appliquée pour différents objectifs, tels que :
— Limiter l'accès à une machine spécifique sur le réseau
— Restreindre le nombre de machines pouvant se connecter à un port du commutateur

2.2.1 Fonctionnement général

Le Port Security permet de contrôler les adresses MAC autorisées sur un port. Il offre plusieurs modes de configuration :
— **Apprentissage statique** : L'administrateur configure manuellement les adresses MAC autorisées sur le port.
— **Apprentissage dynamique** : Le commutateur apprend automatiquement les adresses MAC des dispositifs connectés, ces adresses sont stockées en mémoire et perdues en cas de redémarrage.
— **Apprentissage sticky** : Le commutateur apprend automatiquement les adresses MAC et les conserve dans la configuration en cours, ces adresses peuvent être sauvegardées permettant une persistance après un redémarrage.

Lorsqu'une adresse MAC non autorisée est détectée sur un port sécurisé, le commutateur peut réagir selon différents modes de violation :
— **Protect** : Les trames provenant des adresses MAC non autorisées sont ignorées, sans notification.
— **Restrict** : Les trames des adresses non autorisées sont ignorées et une alerte est générée, enregistrant l'événement dans les journaux du système.
— **Shutdown** : Le port est désactivé (passé en état err-disable), nécessitant une intervention manuelle ou une temporisation configurée pour le réactiver.

2.2.2 Avantages principaux

— **Sécurité renforcée** : En limitant le nombre et les types de dispositifs pouvant se connecter à un port, le Port Security réduit les risques d'accès non autorisés.
— **Protection contre les attaques** : Il aide à prévenir des attaques telles que le MAC flooding, où un attaquant inonde le commutateur avec de multiples adresses MAC pour saturer sa table de correspondance.
— **Simplicité de configuration** : Le Port Security est relativement simple à mettre en œuvre et ne nécessite pas d'infrastructure supplémentaire, ce qui le rend accessible pour des déploiements rapides.

— **Flexibilité** : Avec les modes d'apprentissage dynamique et sticky, il s'adapte aux environnements où les dispositifs peuvent changer, tout en maintenant un niveau de sécurité adéquat.

3 Comparaison des deux mécanismes

Critère	Port Security	IEEE 802.1X
Principe de fonctionnement	Limite l'accès aux ports du commutateur en se basant sur les adresses MAC autorisées.	Contrôle l'accès au réseau via une authentification basée sur le port, généralement en utilisant un serveur RADIUS.
Niveau de sécurité	Sécurité de base ; vulnérable au spoofing d'adresses MAC.	Sécurité avancée avec authentification mutuelle ; résiste mieux aux tentatives d'usurpation.
Gestion des utilisateurs	Configuration manuelle des adresses MAC autorisées ; peu évolutif pour de grands réseaux.	Gestion centralisée des identités via un serveur AAA (Authentification, Autorisation, Accounting) ; adapté aux grandes infrastructures.
Détection des intrusions	Détecte les connexions non autorisées basées sur des adresses MAC inconnues.	Offre une détection plus fine des accès non autorisés grâce à l'authentification utilisateur/machine.
Complexité de mise en œuvre	Relativement simple à configurer sur des petits réseaux.	Nécessite une infrastructure supplémentaire (serveur RADIUS) et une configuration plus complexe.
Flexibilité	Moins flexible ; chaque changement d'appareil nécessite une mise à jour manuelle des adresses MAC autorisées.	Plus flexible ; les politiques d'accès peuvent être modifiées de manière centralisée sans intervention sur chaque commutateur.

Table 1 – Comparaison entre Port Security et IEEE 802.1X

4 Scénarios et analyses

Pour illustrer l'interaction entre IEEE 802.1X et Port Security, examinons deux scénarios concrets mettant en évidence leur complémentarité dans la sécurisation des réseaux.

Scénario 1 : Machine malveillante authentifiée via 802.1X, bloquée par Port Security
Contexte : Une entreprise utilise l'authentification 802.1X pour contrôler l'accès à son réseau local. Une machine malveillante parvient à obtenir des identifiants valides et réussit l'authentification 802.1X.

Déroulement :

1. La machine malveillante se connecte physiquement au réseau et fournit des identifiants valides.
2. Le serveur d'authentification (par exemple, RADIUS) valide ces identifiants, et l'accès réseau est accordé via 802.1X.
3. Cependant, Port Security est configuré pour n'autoriser qu'une adresse MAC spécifique ou un nombre limité d'adresses MAC sur ce port.
4. La machine malveillante, avec une adresse MAC différente ou en dépassant le nombre autorisé, déclenche une violation de Port Security.
5. En réponse, le commutateur peut désactiver le port, générer une alerte ou bloquer le trafic de cette adresse MAC, empêchant ainsi l'accès réseau malgré l'authentification réussie.

Ce scénario démontre que, même si une machine malveillante réussit l'authentification 802.1X, Port Security ajoute une couche supplémentaire de protection en contrôlant les adresses MAC autorisées sur chaque port, limitant ainsi les risques liés à l'utilisation d'identifiants compromis.

Scénario 2 : Usurpation d'adresse MAC et limitations des mécanismes de sécurité
Contexte : Un attaquant tente d'accéder au réseau en usurpant l'adresse MAC d'un appareil autorisé.

Déroulement :

1. L'attaquant configure son appareil avec l'adresse MAC d'un dispositif légitime.
2. Cas 1 : Réseau protégé par Port Security uniquement :
   — Si l'adresse MAC usurpée est autorisée sur le port, l'attaquant obtient l'accès réseau.
   — Port Security, basé uniquement sur les adresses MAC, ne détecte pas l'usurpation.
3. Cas 2 : Réseau protégé par 802.1X uniquement :
   — L'attaquant doit fournir des identifiants valides pour réussir l'authentification.
   — Sans ces identifiants, l'accès est refusé, même avec une adresse MAC usurpée.
4. Cas 3 : Réseau combinant 802.1X et Port Security :
   — L'attaquant doit à la fois usurper une adresse MAC autorisée et fournir des identifiants valides.
   — Cette double exigence complexifie l'attaque et renforce la sécurité globale.

L'usurpation d'adresse MAC exploite les faiblesses des mécanismes basés uniquement sur les adresses MAC, comme Port Security. L'intégration de 802.1X ajoute une couche d'authentification robuste, rendant l'usurpation seule insuffisante pour accéder au réseau. Cependant, il est important de noter que des vulnérabilités peuvent exister dans certaines implémentations de 802.1X, notamment en cas d'attaques de type "man-in-the-middle" ou d'usurpation de messages EAPOL-Logoff. Ainsi, la combinaison des deux mécanismes offre une sécurité renforcée, mais il est essentiel de rester vigilant quant aux limitations potentielles et de mettre en place des mesures complémentaires, telles que l'utilisation de certificats numériques et la surveillance active du réseau.

Ces scénarios illustrent comment l'utilisation conjointe de 802.1X et de Port Security peut renforcer la sécurité réseau en ajoutant des couches de protection complémentaires, tout en reconnaissant les limitations inhérentes à chaque mécanisme.

5 Conclusion

En conclusion, la sécurisation des réseaux locaux repose sur l'utilisation judicieuse de mécanismes tels que **Port Security** et **IEEE 802.1X**. Chacun offre des avantages spécifiques :

— **Port Security** permet de contrôler l'accès au réseau en limitant le nombre d'adresses MAC autorisées sur un port, offrant une protection efficace contre certaines attaques basées sur le trafic réseau.
— **IEEE 802.1X** fournit une authentification robuste au niveau du port, s'assurant que seuls les utilisateurs et dispositifs autorisés peuvent accéder aux ressources réseau, renforçant ainsi la sécurité globale.

L'intégration de ces deux technologies permet de créer une défense en profondeur, combinant le contrôle d'accès basé sur les adresses MAC et une authentification utilisateur solide. Cependant, il est essentiel de reconnaître les limitations potentielles de chaque mécanisme et de les configurer correctement pour éviter des conflits ou des failles de sécurité.

En somme, une approche combinée et bien configurée de **Port Security** et **IEEE 802.1X** constitue une stratégie efficace pour protéger les réseaux locaux contre les accès non autorisés et les menaces potentielles.

6 Bibliographie et sources utilisées

— The History of RADIUS Authentication Protocol & IEEE 802.1X
— Intro to Networking: AAA, 802.1X / EAP, RADIUS
— Configuring 802.1X
— Switchport Port-Security (Sécurité sur les ports) Cisco en IOS

— Guide d'utilisation de 802.1X
— IEEE 802.1X