

## *MOOC Réseaux Locaux*

### *Les réseaux locaux en entreprise*

## **La sécurité des réseaux locaux**

### Objectifs

Cette leçon a pour but de présenter les outils de base de la sécurité des réseaux locaux.

### Prérequis

Bonne connaissance des réseaux locaux

### Connaissances

Principales techniques utilisées pour assurer la sécurité des réseaux locaux.

### Compétences




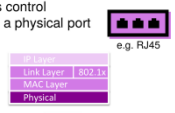

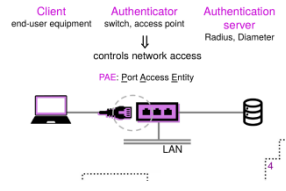
Analyser les outils de sécurisation des réseaux locaux.

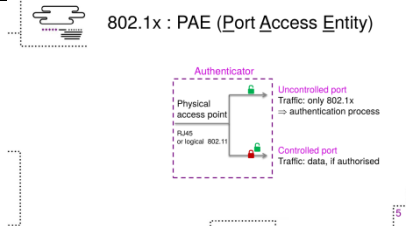
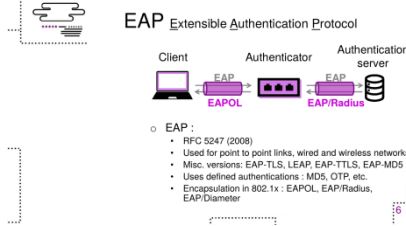
### Évaluation des connaissances

Décrire les techniques de sécurisation des réseaux locaux.

### Évaluation des compétences

Dérouler un scénario de sécurisation d'un réseau local.

 <p><b>Enterprise networks</b> <i>Lan security</i></p> <p>Samiha Ayed</p>	
 <p><b>Objectives</b></p> <ul style="list-style-type: none"> <li>802.1x standard <ul style="list-style-type: none"> <li>802.1x architecture</li> <li>EAP authentication protocol</li> </ul> </li> </ul>	<p>Dans cette vidéo, j'aborde avec vous la norme IEEE 802.1. Je vous présente les différents composants de l'architecture proposée par ce standard ainsi que le protocole d'authentification EAP.</p>
 <p><b>The 802.1x standard</b></p> <ul style="list-style-type: none"> <li>IEEE - June 2001</li> <li>Authentication before any auto-configuration (IP...)</li> <li>Access control through a physical port</li> </ul> 	<p>La norme 802.1x a été définie par l'IEEE en juin 2001. L'idée de base de ce standard est comment un utilisateur qui rejoint le réseau peut être authentifié et autorisé à rejoindre ce réseau avant même d'avoir une adresse IP.</p> <p>Ce contrôle d'accès est basé sur le port. Ici on parle de port de connectivité physique comme par exemple le RJ45 pour Ethernet. Pour ce contrôle d'accès lors de la phase d'authentification, nous nous plaçons au niveau de la couche 2.</p>
 <p><b>802.1x entities</b></p> 	<p>Le standard définit trois composants qui constituent son architecture :</p> <ul style="list-style-type: none"> <li>le client c'est le système à authentifier qui peut être un poste de travail ou un serveur</li> <li>l'authentificateur qui autorise l'accès au réseau mais n'a pas la capacité de déterminer si une machine est autorisée ou pas à joindre le réseau. Dans la plupart des implémentations actuelles, le système authentificateur est un équipement réseau par exemple un commutateur Ethernet une borne d'accès sans fil ou un commutateur routeur IP</li> <li>le troisième composant est le serveur d'authentification qui est l'entité qui décide si l'accès est permis ou pas et informe l'authentificateur de cette décision. Le serveur d'authentification est typiquement un serveur radius ou tout autre équipement capable de faire de l'authentification.</li> </ul> <p>Le système authentificateur contrôle l'accès au réseau via le point d'accès physique au réseau nommé PAE (Port Access Entity). C'est au niveau du PAE que portent l'essentiel des modifications introduites par le protocole 802.1x.</p>

 <p>802.1x : PAE (Port Access Entity)</p>	<p>La principale innovation amenée par le standard 802.1x consiste à scinder le port d'accès physique au réseau qui peut être matérialisée par un câble RJ45 ou le port logique 802.11 en deux ports logiques qui sont connectés en parallèle sur le port physique.</p> <p>Le premier port logique est toujours accessible et dit non contrôlé mais il ne gère que les trames spécifiques à 802.1x et c'est à travers lequel on assure le processus d'authentification.</p> <p>Le deuxième port est dit contrôlé et peut prendre deux états : ouvert ou fermé et c'est le port qu'on utilise pour le transfert des données, une fois le client authentifié et autorisé à accéder au réseau.</p>
 <p>EAP Extensible Authentication Protocol</p> <ul style="list-style-type: none"> <li>Client</li> <li>Authenticator</li> <li>Authentication server</li> </ul> <p>○ EAP :</p> <ul style="list-style-type: none"> <li>• RFC 5247 (2008)</li> <li>• Used for point to point links, wired and wireless networks</li> <li>• Misc. versions: EAP-TLS, LEAP, EAP-TTLS, EAP-MD5</li> <li>• Uses defined authentications : MD5, OTP, etc.</li> <li>• Encapsulation in 802.1x : EAPOL, EAP/RADIUS, EAP Diameter</li> </ul>	<p>Le standard 802.1x ne crée pas un nouveau protocole d'authentification mais s'appuie sur les standards existants. Le dialogue entre le client le système authentificateur et le serveur d'authentification se fait en utilisant le protocole EAP défini par la RFC 5247.</p> <p>Ce protocole a été défini pour être utilisé pour des liaisons point à point pour des réseaux filaires ou aussi pour des réseaux sans fil. Il existe plusieurs variantes du protocole EAP comme EAP-TLS, LEAP, EAP-TTLS pour EAP-MD5 qui assurent des différentes propriétés de sécurité.</p> <p>Concernant les méthodes d'authentification, EAP utilise des méthodes d'authentification prédéfinies comme le MD5 et le OTP. EAP est utilisable avec différents protocoles de niveau 2 (donc niveau liaison) grâce au mécanisme d'encapsulation.</p> <p>Par exemple dans le cas où le client et le système authentificateur sont connectés par Ethernet, les paquets EAP sont transportés dans des trames Ethernet spécifiques EAPOL (pour EAP Over Lan). Le dialogue entre le système authentificateur et le serveur d'authentification se fait par une simple ré-encapsulation des paquets EAP dans un format qui convient aux serveurs d'authentification par exemple le format RADIUS dans notre cas.</p>

<div data-bbox="183 190 271 235" data-label="Image"></div> <div data-bbox="378 197 466 226" data-label="Section-Header"> <h3>Example</h3> </div> <div data-bbox="327 230 596 416" data-label="Diagram"> </div>	<p>Pour assurer la communication entre les différents composants, l'EAP définit quatre types de paquets : request response, succes, et fail.</p> <p>Suivons un exemple de communication.</p> <ul style="list-style-type: none"> <li>- Alice branche son câble rj45 pour se connecter au réseau local donc une requête EAP start est envoyée à l'authentificateur qui lui pose la question sur l'identité d'Alice à travers un message EAP request.</li> <li>- Alice répond en envoyant son identité dans une EAP response.</li> <li>- Ayant reçu l'identité d'Alice, l'authentificateur informe le serveur d'authentification de la présence d'Alice et lui demande si elle est autorisée à accéder au réseau.</li> <li>- Le serveur radius demande si Alice peut fournir des informations privées comme son mot de passe par exemple.</li> <li>- L'authentificateur transfère la requête vers Alice qui envoie son mot de passe dans une EAP response.</li> <li>- L'authentificateur transfère la réponse au serveur radius et reçoit son autorisation pour que Alice accède au réseau.</li> <li>- L'authentificateur envoie finalement cette autorisation à Alice dans un EAP success. Dans ce cas d'authentification réussie, le système authentificateur débloquera le port contrôlé.</li> </ul>
<div data-bbox="183 1292 271 1337" data-label="Image"></div> <div data-bbox="365 1303 474 1330" data-label="Section-Header"> <h3>Conclusion</h3> </div> <div data-bbox="325 1346 547 1456" data-label="List-Group"> <ul style="list-style-type: none"> <li>o The 802.1x standard <ul style="list-style-type: none"> <li>• Ensures at port level a link layer authentication</li> <li>• Strengthens the security of wired networks</li> <li>• Is used in 802.11i for Wi-Fi security</li> </ul> </li> </ul> </div>	<p>En conclusion le standard 802.1x existe principalement pour assurer l'authentification à travers les ports physiques. Cette norme est utile dans le cadre des réseaux filaires et elle a également montré son utilité pour la norme 802.11i, dédiée à la sécurité Wi-Fi.</p>