07 Le serveur RADIUS

Module 146

ICT Berufsbildung
Formation professionnelle
Formazione professionale

1. Introduction

Le RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification.

Le protocole RADIUS a été inventé et développé en 1991 par la société Livingston, qui fabriquait des serveurs d'accès au réseau pour des matériels uniquement équipés d'interfaces série.

Janvier 1997 : Première version de RADIUS
RFC 2058 (authentication) et 2059 (accounting).

Avril 1997 : Deuxième version de RADIUS

RFC 2138 (authentication) et 2139 (accounting).

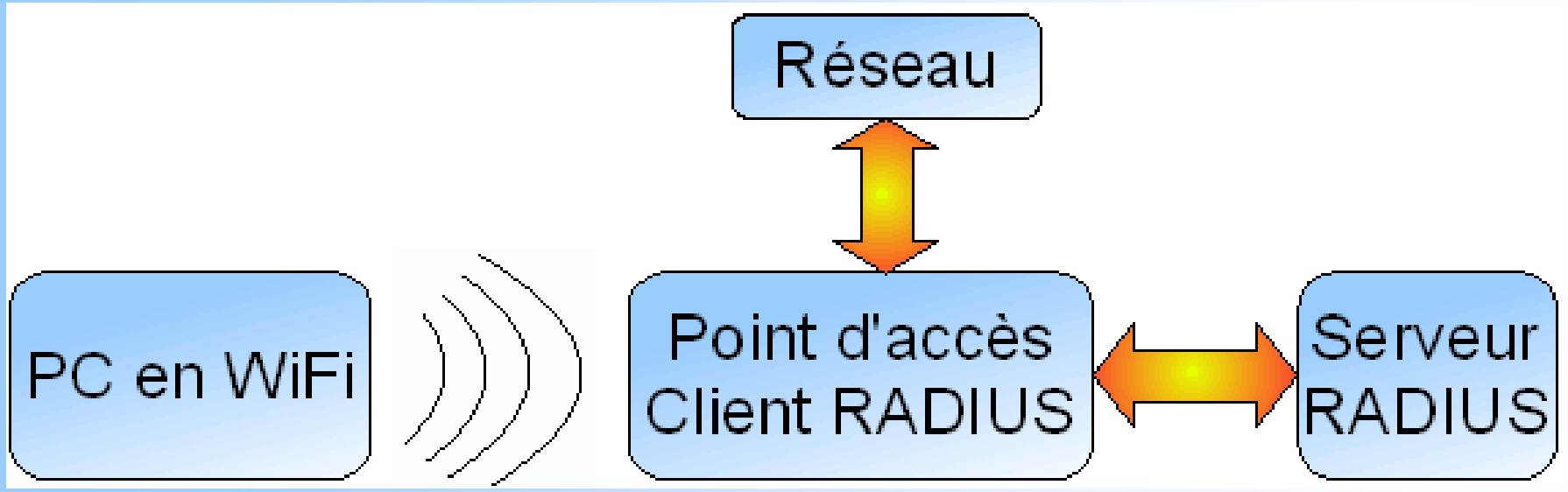
Juin 2000 : La dernière version de RADIUS

RFC 2865 (authentication) et 2866 (accounting).

2. Exemples d'utilisation

Le RADIUS peut être utilisé par les FAI pour identifier les clients à l'aide d'un serveur LDAP;

ou utilisé par des points d'accès WiFi pour accéder à un réseau



3. Le protocole RADIUS

Il existe 4 types de paquets pour effectuer une authentification RADIUS :

- **Access-Request :** envoyé par le NAS contenant les informations sur le client qui souhaite se connecter (login/mot de passe, adresse MAC…)
- **Access-Accept :** Envoyé par le serveur pour autorisé la connexion si la vérification des informations est correct.
- **Access-Reject :** Envoyé par le serveur pour refuser une connexion en cas d'échec de l'authentification ou pour mettre fin à une connexion.
- **Access-Challenge :** Envoyé par le serveur pour demander la réémission d'un access-request ou des informations complémentaires.

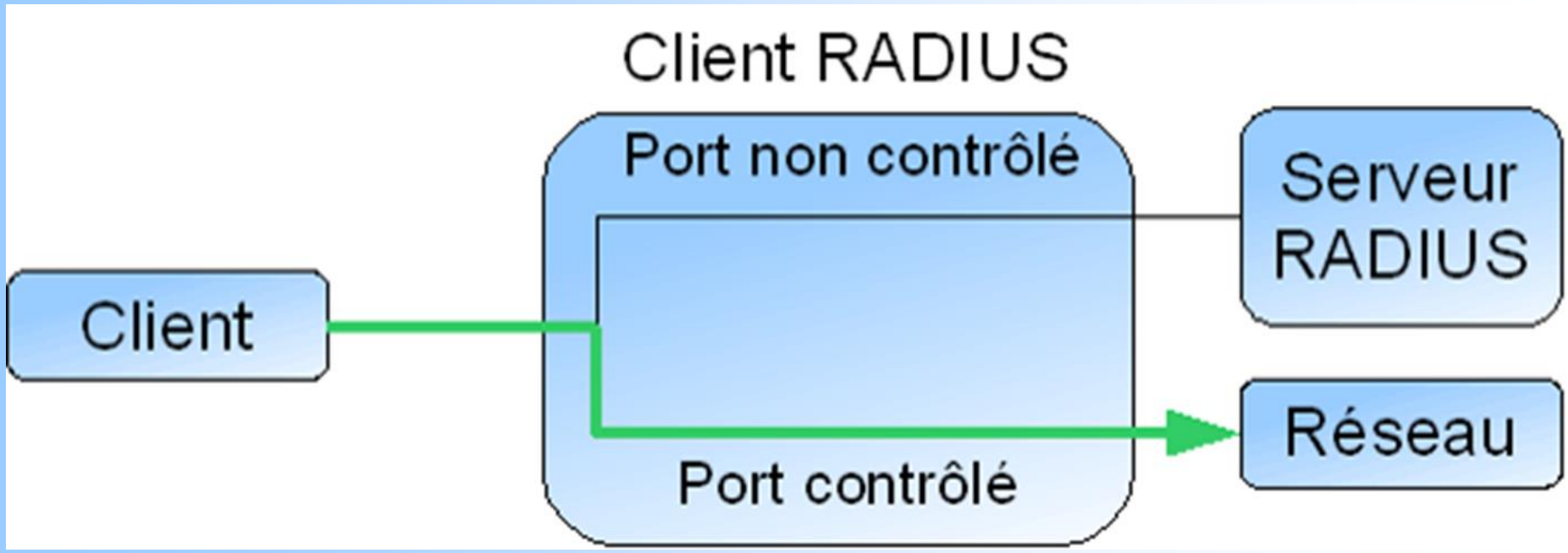
4. Le protocole 802.1x

- Le protocole 802.1X a été mis au point par l'IEEE en juin 2001.
- 802.1X est un standard lié à la sécurité des réseaux informatiques.
- Il permet de contrôler l'accès aux équipements d'infrastructures réseau.
- Il a pour but d'authentifier un client afin de lui autoriser l'accès à un réseau.
- On utilise le protocole EAP (Extensible Authentication Protocol) et un serveur d'authentification qui est généralement un serveur RADIUS
- Le serveur RADIUS va authentifier chaque client qui se connecte au réseau sur un port.

5. Le fonctionnement du protocole 802.1x

Au début de la connexion, le port est dans l'état non contrôlé.

Seuls les paquets 802.1X permettant d'authentifier le client sont autorisés.

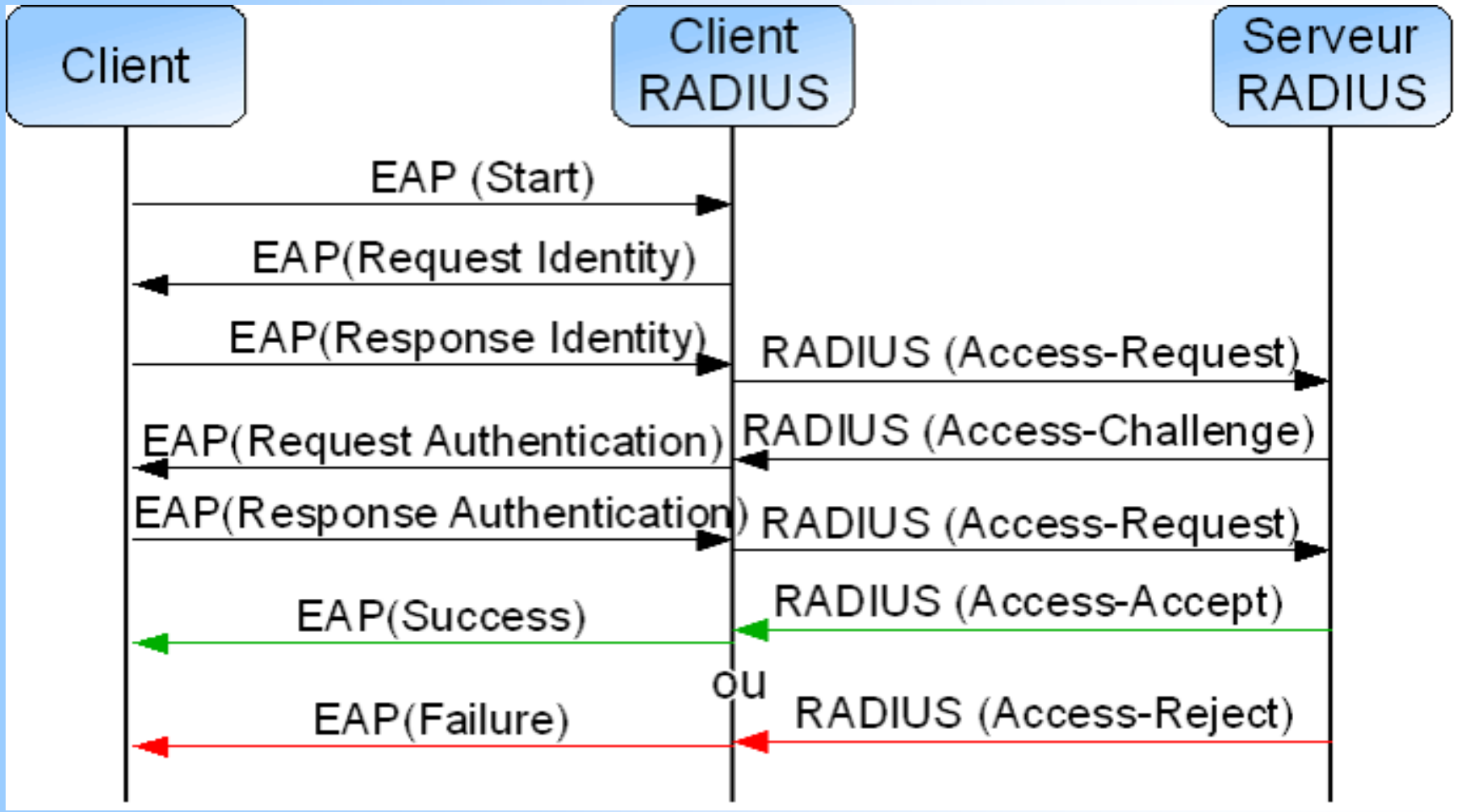


Une fois l'authentification effectuée, le port passe dans l'état contrôlé.

Alors, tous les flux du client sont acceptés et le client peut accéder aux ressources partagées.

5. Le fonctionnement du protocole 802.1x

Etapes d'authentification :



6. Les faiblesses de 802.1X :

- Le protocole 802.1X a été prévu pour établir une connexion physique.
  Donc l'insertion d'un hub permet de faire bénéficier d'autres personnes de l'ouverture du port Ethernet, tout en restant transparent pour le 802.1X
- Il est possible de configurer les équipements réseaux de façon à bloquer le port Ethernet si l'adresse MAC à changé.
- Il est également possible de faire des attaques par écoute, rejeu et vol de session.

7. Le protocole EAP

EAP signifie Extensible Authentication Protocol.

C’est un protocole de communication réseau qui est constitué d'un échange de trames dans un format spécifique à EAP pour réaliser l'authentification d'un partenaire.

C’est est un protocole de communication réseau embarquant de multiples méthodes d'authentification.

Dans notre cas, c’est lui qui fait le lien entre le client (supplicant) et le client RADIUS (Authenticator).

7. Les principaux type d'EAP

- **EAP-TLS (Transport Layer Security) :** Authentification par certificat du client et du serveur
- **EAP-TTLS (Tunneled Transport Layer Security) :** Authentification par certificat et mot de passe grâce à la génération d'un tunnel sécurisé
- **EAP-MD5 :** Authentification avec mot de passe
- **PEAP (Protected EAP) :** Authentification avec mot de passe via une encapsulation sécurisée
- **LEAP (protocole Cisco) :** Authentification avec mot de passe via une encapsulation sécurisée

8. Diameter

Le Diameter est un protocole d'authentification, successeur du protocole RADIUS.

Il est notamment utilisé dans le cœur des réseaux de téléphonie mobile pour accéder aux bases de données HLR et HSS permettant d'identifier, d'authentifier et de localiser les abonnés mobiles 3G et LTE /4G.

Contrairement à RADIUS, son nom est un jeu de mot, diameter, signifiant diamètre en anglais, qui est le double du rayon, radius en anglais.

Quelques différences avec RADIUS :

Il utilise le protocole TCP,
il peut utiliser le transport réseau sécurisé (IPsec ou TLS),
La taille des attributs est augmentée,
il est mieux adapté au roaming.

9. Conclusion

Avantages :

- Sécurité
- Fiabilité
- Centralisation de l'authentification

Inconvénients :

- Lourd à mettre en place
- Limité à 254 octets par attribut