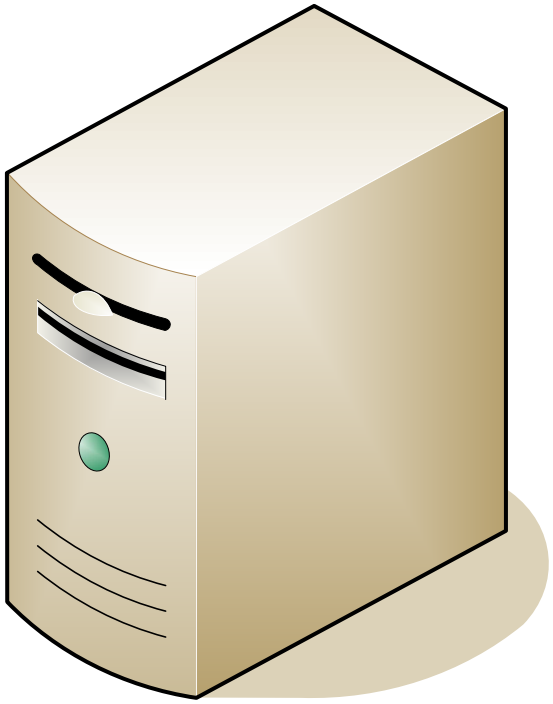
RADIUS

Remote
Authentication
Dial
In
User
Service



GAUTHIER Julien

INGÉNIEURS 2000

Sommaire

- Qu’est ce que RADIUS ?
- Historique
- Exemples d’utilisation de RADIUS
- Le protocol RADIUS
- Le protocol 802.1X
- Serveur RADIUS open source
- Successeur de RADIUS
- Conclusion

Qu’est ce que RADIUS ?

Authentification (authentication):

- Protocole d'authentification à distance
- Centralisation des données d’authentification
- Gestion des connexions utilisateurs à des services distants

Comptabilisation (accounting):

- Utilisé pour assurer la journalisation et la facturation

Historique

Projet de la société Livingston sur un protocol d'authentification standard

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

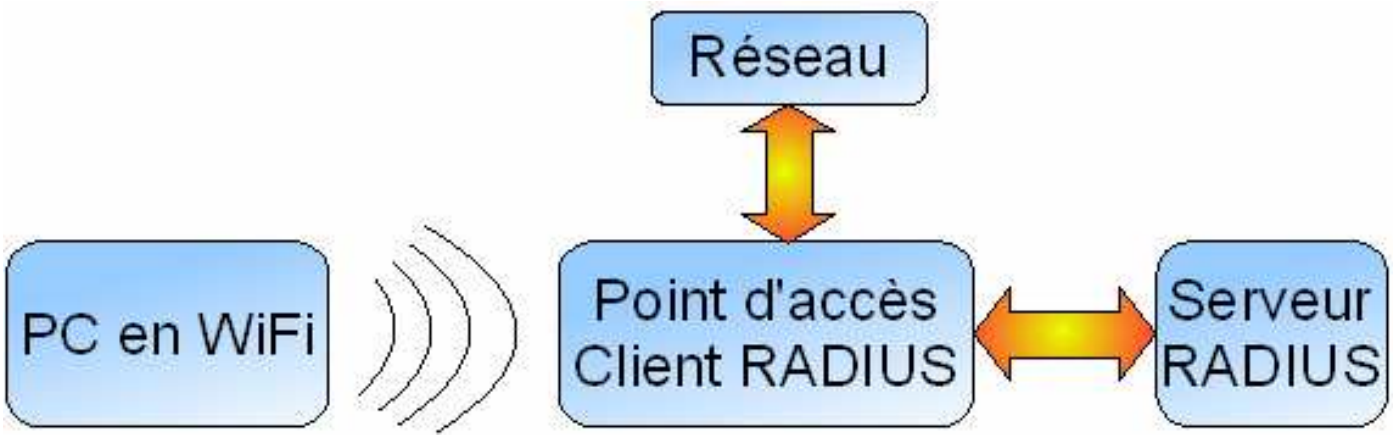
Avril 1997 : Deuxième version de RADIUS
RFC 2138 (authentication) et 2139 (accounting).

Juin 2000 : La dernière version de RADIUS
RFC 2865 (authentication) et 2866 (accounting).

Exemples d’utilisation de RADIUS

- Utilisé par les FAI pour identifier les clients à l’aide d’un serveur LDAP

Exemples d’utilisation de RADIUS



Supplicant

Authenticator ou NAS
(Network Access Serveur)

Authentication
Serveur

-Utilisé par des points d’accès WiFi pour accéder à un réseau

-Utilisation d’un secret partagé entre le serveur et le client

Le protocol RADIUS

Pourquoi UDP ?

- Permet la réémission d’une demande d’authentification à un serveur secondaire si le serveur primaire ne répond pas
- RADIUS est un protocol sans état.
- UDP simplifie la mise en œuvre du serveur.
- RADIUS n’exige pas une détection "sensible" de la perte de données

Le protocol 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**

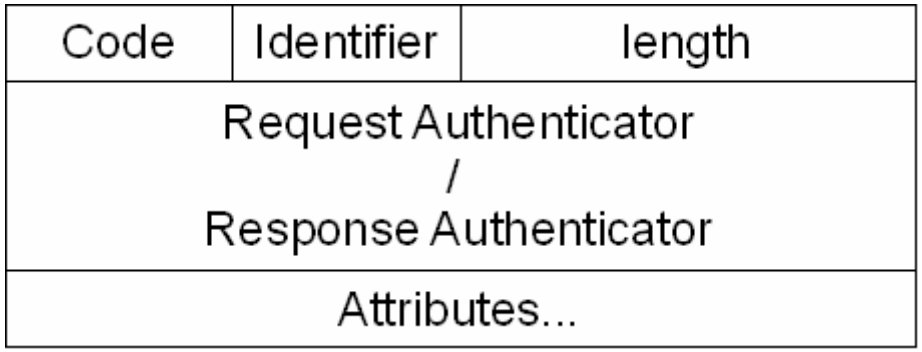
  Envoyé par le serveur pour refuser une connexion en cas d'échec de l'authentification ou pour mettre fin à une connexion.

- **Access-Challenge**

  Envoyé par le serveur pour demander la réémission d'un access-request ou des informations complémentaires.

Le protocol RADIUS

Format des trames :



Code (1 octet):
1 : access-request
2 : access-accept
3 : access-reject
4 : accounting-request
5 : accounting-response
11 : access-challenge

Identifier (1 octet) :
- Unique pour chaque authentification
- Identique pour une retransmission

Length (2 octets):
- Taille total du message (de 20 à 4096 octets)

Request Authenticator (16 octets):

Un nombre aléatoire unique

Response Authenticator (16 octets):

MD5 (Code + ID + Length + RequestAuth + Attributes + Secret)

Le protocol RADIUS

Les attributs :

Type (1 octet):
1 : User-Name
2 : User-Password
3 : CHAP-Password
4 : NAS-IP-Address
5 : NAS-Port
6 : Service-Type …

Length (1 octets):
- Taille total du message (max 254 octets)

Value (1-253 octets):
text 1-253 octets
string 1-253 octets
address 32 bit
integer 32 bit
time 32 bit

User-Password :

Le mot de passe est coupé en blocks de 16 octets : p1, p2,…

c1 = p1 XOR MD5(Secret + Request Authenticator)
c2 = p2 XOR MD5(Secret + c1)
…

Le mot de passe encodé est la concaténation de : c(1)+c(2)+...

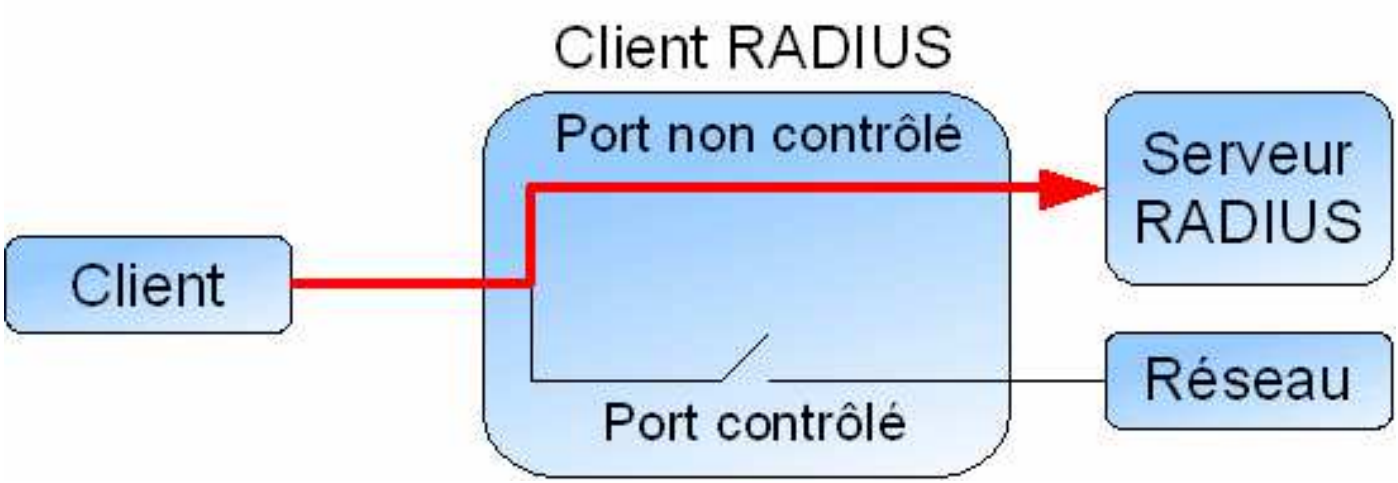
Le protocol 802.1X

- Le protocol 802.1X a été mis au point par l'IEEE en juin 2001. Il a pour but d'authentifier un client (en filaire ou en WiFi) afin de lui autoriser l'accès à un réseau.

- On utilise le protocol EAP(Extensible Authentication Protocol) et un serveur d'authentification qui est généralement un serveur RADIUS

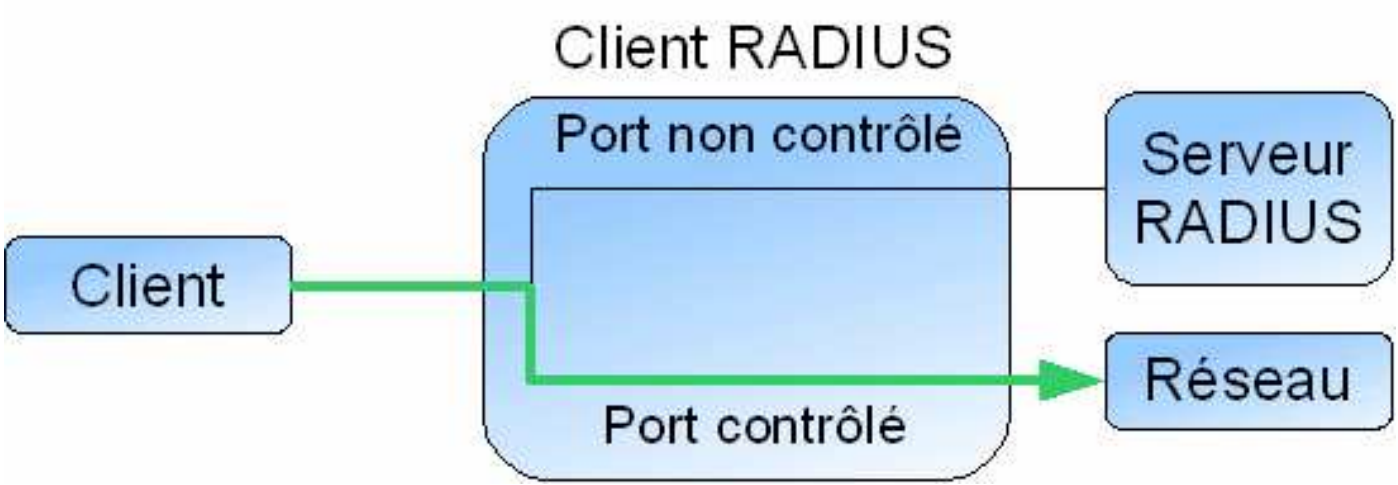
- Le serveur RADIUS va authentifier chaque client qui se connecte au réseau sur un port.

Le protocol 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.

Le protocol 802.1X



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.

Le protocol 802.1X

Les principaux types d'EAP :

EAP-TLS (Transport Layer Security)
Authentification par certificat du client et du serveur

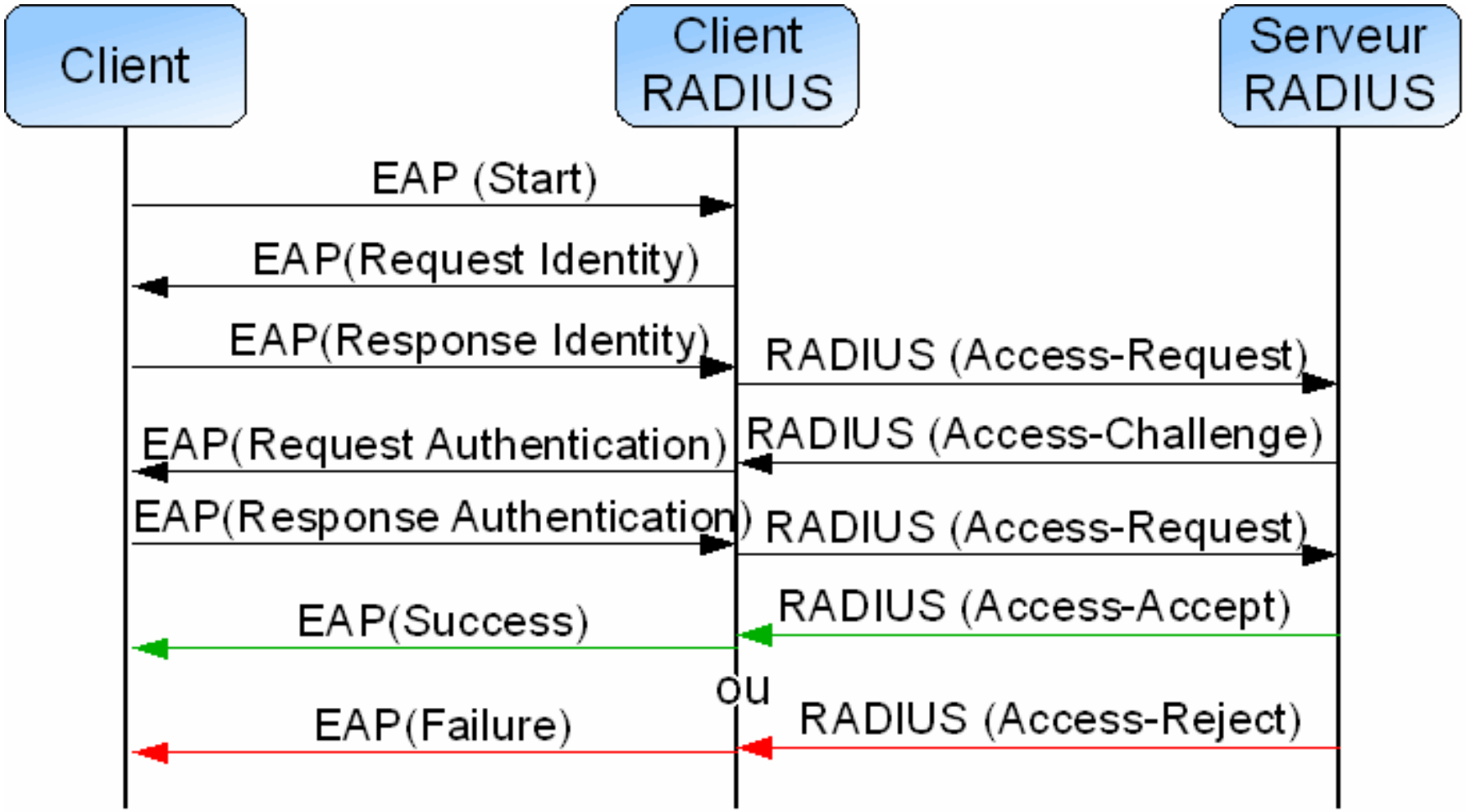
EAP-TTLS (Tunneled Transport Layer Security) :
Authentification par certificat et mot de passe grâce à la génération d'un tunnel sécurisé

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

Le protocol 802.1X



Etapes d’authentification 802.1X

Le protocol 802.1X

Les faiblesses de 802.1X :

- Le protocol 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.

serveur RADIUS open source

Méthodes	Free RADIUS	Cistron RADIUS	ICRadius	XTRadius	Open RADIUS	GNU-Radius	YARD-Radius
EAP/SIM							
EAP/TLS							
EAP/TTLS							
EAP/MD5							
CHAP							
PAP							
PEAP							
Cisco-LEAP							
Couple login/mot de passe							

serveur RADIUS open source

Support d' authentification	Free RADIUS	Cistron RADIUS	ICRadius	XTRadius	Open RADIUS	GNU-Radius	YARD-Radius
PAM	■	■	■		■	■	■
Unix	■	■	■	■	■	■	■
MySQL	■		■		■	■	
PostgreSQL	■				■	■	
Oracle	■						
LDAP	■				■		
Perl DBI	■		■				
Perl DBD	■		■				
Berkeley DB	■		■	■		■	■
SMB	■				■		
ODBC	■					■	

Successeur de RADIUS

Diameter est le successeur de RADIUS, il est généralement compatibles avec RADIUS et EAP.

Quelques différences avec RADIUS :

- Utilise le protocol TCP
- Peut utiliser le transport réseau sécurisé (IPsec ou TLS)
- La taille des attributs est augmentée
- Mieux adapté au roaming
- Diameter contient certains attributs qui sont dans EAP-TTLS

Conclusion

Avantages :

- Sécurité
- Fiabilité
- Centralisation de l’authentification

Inconvénients :

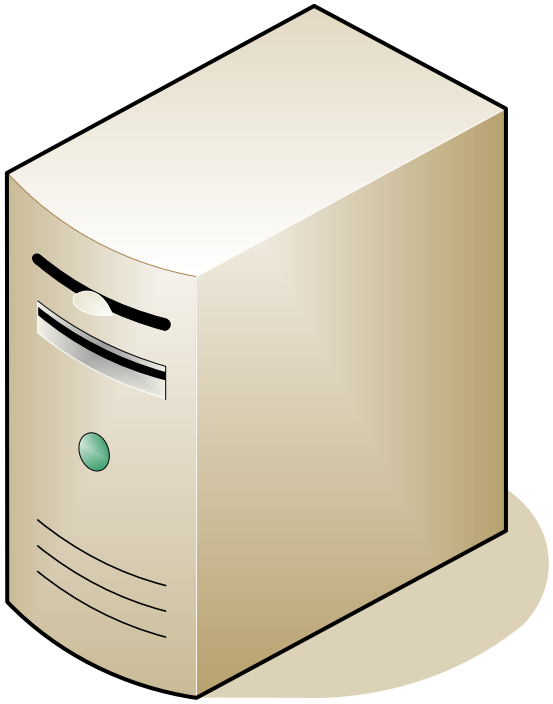
- Lourd à mettre en place
- Limité à 254 octets par attribut

Sources

http://www.commentcamarche.net/authentification/radius.php3
http://www.journaldunet.com/solutions/0611/061122-qr-radius.shtml
http://fr.wikipedia.org/wiki/Radius_(informatique)
http://en.wikipedia.org/wiki/Diameter_(protocol)
http://en.wikipedia.org/wiki/802.1x
http://www.nantes-wireless.org/
http://www.supinfo-projects.com/
http://raisin.u-bordeaux.fr/IMG/pdf/radius.pdf
http://raisin.u-bordeaux.fr/IMG/pdf/Protocoles-auth-2pages.pdf
http://tools.ietf.org/html/rfc2865
http://tools.ietf.org/html/rfc2866

RADIUS

Remote
Authentication
Dial
In
User
Service



GAUTHIER Julien

INGÉNIEURS 2000