Réseaux

Chapitre 8 - Le protocole RADIUS

Claude Duvallet

Université du Havre
UFR Sciences et Techniques
25 rue Philippe Lebon - BP 540
76058 LE HAVRE CEDEX
Claude.Duvallet@gmail.com

Objectifs du cours

- Présenter le principe du serveur RADIUS.
- Présenter WPA
- Présenter 802.1x
- Présenter EAP

Plan de la présentation

Références bibliographiques

- **Serge Bordères.** *Authentification réseau avec Radius : 802.1x, EAP, FreeRadius.* Eyrolles. 2006.
- **Jonathan Hassell.** *Radius.* O'Reilly. 2002.

Principes généraux de Radius

- Protocole standard d'authentification, initialement mis au point par Livingston.
- Défini au sein des RFC 2865 et 2866.
- Fonctionnement basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau.
- Protocole de prédilection des fournisseurs d'accès à internet :
  - relativement standard,
  - propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.
- Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée.

Principe de fonctionnement de Radius

- RADIUS repose principalement :
  - sur un serveur (le serveur RADIUS),relié à une base d'identification (base de données, annuaire LDAP, etc.),
  - sur un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur.
- L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré.
- Le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.
- Le serveur traite les demandes d'authentification en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine.
  - un serveur RADIUS dispose pour cela d'un certain nombre d'interfaces ou de méthodes.

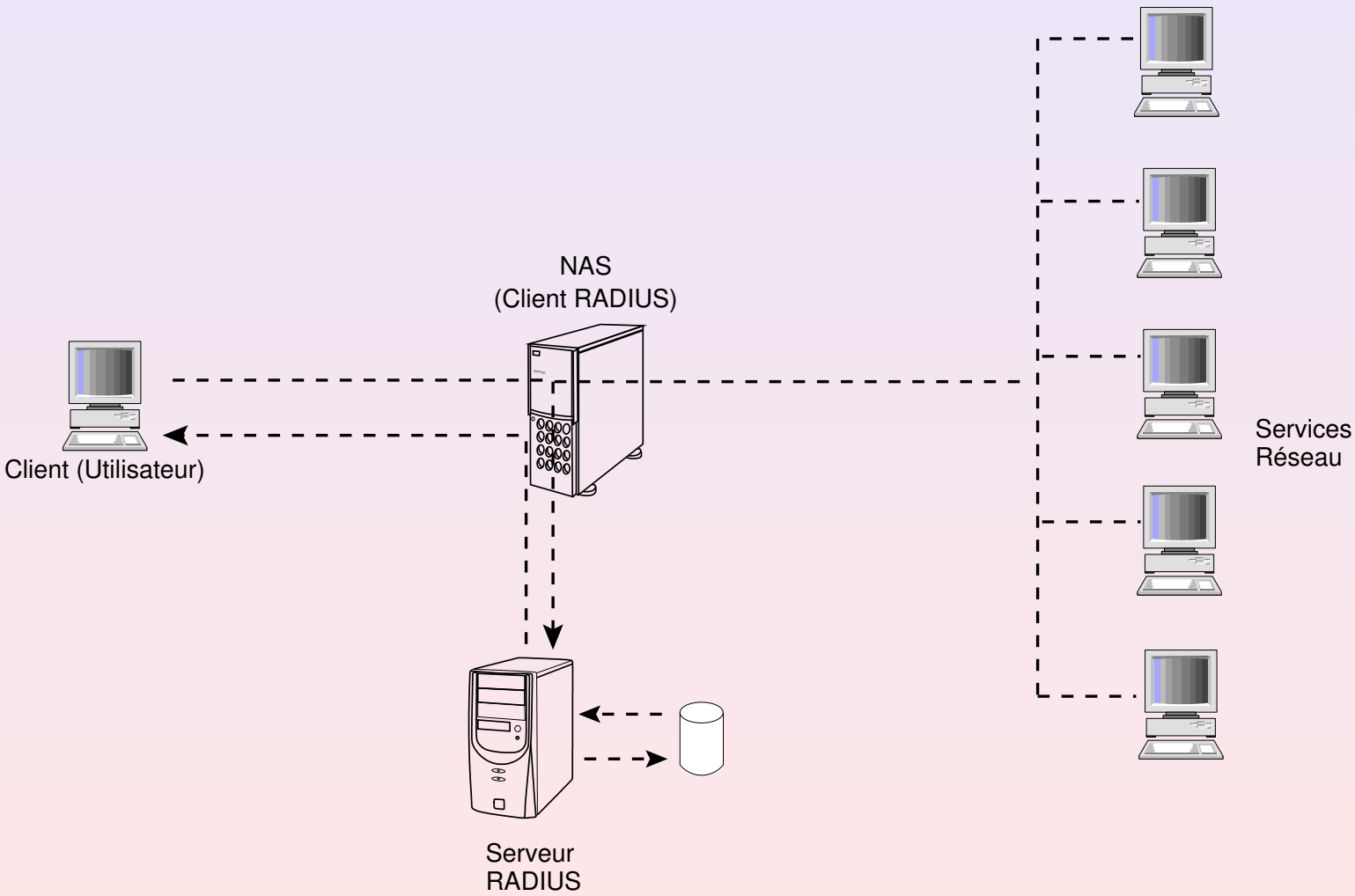
Scénario de fonctionnement (1/2)

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
- Le NAS achemine la demande au serveur RADIUS.
- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur.
- Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
  - **ACCEPT** : l'identification a réussi.
  - **REJECT** : l'identification a échoué.
  - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi ».

Scénario de fonctionnement (2/2)

- Une autre réponse est possible : **CHANGE PASSWORD** où le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.
- Change-password est un attribut VSA (Vendor-Specific Attributes), c'est-à-dire qu'il est spécifique à un fournisseur.
- Suite à cette phase dit d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

Schéma de fonctionnement du protocole RADIUS



Protocoles de mot de passe

- RADIUS connaît nativement deux protocoles de mot de passe :
  - PAP (échange en clair du nom et du mot de passe),
  - CHAP (échange basé sur un hachage de part et d'autre avec échange seulement du 'challenge').
- Le protocole prévoit deux attributs séparés : User-Password et CHAP-Password.
- Depuis, se sont greffées les variations Microsoft : MS-CHAP et MS-CHAP-V2.
- Leur similarité avec CHAP permet de les transporter en RADIUS de la même façon, à l'initiative du serveur et sous réserve bien entendu de possibilité de transport de bout en bout du supplicant au client Radius, du client au serveur Radius et enfin du serveur Radius à la base de données d'identification.

Limitations du protocole RADIUS (1/3)

- RADIUS a été conçu pour des identifications par modem, sur des liaisons lentes et peu sûres :
  - c'est la raison du choix du protocole UDP.
  - ce choix technique d'un protocole non agressif conduit à des échanges laborieux basés sur des temporisations de réémission, des échanges d'accusés de réception.

  $\Rightarrow$ Diameter (qui devrait remplacer RADIUS) utilise TCP ou STCP.
- RADIUS base son identification sur le seul principe du couple nom/mot de passe :
  - parfaitement adapté à l'époque (1996),
  - cette notion a dû être adaptée

    Exemple : pour l'identification des terminaux mobiles par leur numéro IMEI ou par leur numéro d'appel (Calling-Station-ID en Radius) sans mot de passe (alors que la RFC interdit le mot de passe vide !).

Limitations du protocole RADIUS (2/3)

- RADIUS assure un transport en clair, seul le mot de passe est chiffré par hachage :
  - la sécurité toute relative du protocole repose sur le seul shared secret et impose la sécurisation des échanges entre le client et le serveur par sécurité physique ou VPN,

  $\Rightarrow$ Diameter peut utiliser IPSec ou TLS.
- RADIUS limite les attributs :
  - gérés sous forme de chaîne "Pascal" avec un octet en tête donnant la longueur, à 255 octets, cohérents avec la notion de nom/mot de passe,
  - mais inadapté à toute tentative d'introduction de biométrie (fond d'œil, empreinte digitale) de cryptographie (certificat),

  $\Rightarrow$ Diameter utilise des attributs sur 32 bits au lieu de 8 (déjà présents dans certaines extensions EAP de RADIUS, notamment TTLS).

Limitations du protocole RADIUS (3/3)

- RADIUS est strictement client-serveur :
  - d'où des discussions et bagarres de protocoles propriétaires quand un serveur doit légitimement tuer une session pirate sur un client,

  $\Rightarrow$ Diameter a des mécanismes d'appel du client par le serveur.
- RADIUS n'assure pas de mécanisme d'identification du serveur :
  - se faire passer pour un serveur est un excellent moyen de récolter des noms et mots de passe,

  $\Rightarrow$ EAP assure une identification mutuelle du client et du serveur.

Le protocole WPA (1/2)

- Objectif : combler les lacunes du protocole WEP
  - Utilisation d'algorithmes peu développés et facilement craquables.
  - Impossibilité d'authentifier un ordinateur ou un utilisateur qui se connecterait au réseau.
- Définition de deux nouvelles méthodes de chiffrement et de contrôle d'intégrité :
  - TKIP (Temporal Key Integrity Protocol) :
    - s'adapte au mieux au matériel existant,
    - utilise RC4 comme algorithme de chiffrement,
    - ajoute un contrôle d'intégrité MIC,
    - introduit un mécanisme de gestion de clés (création de clés dynamiques à intervalle de temps régulier).
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) :
    - plus puissant que TKIP,
    - utilise AES comme algorithme de chiffrement,
    - totalement incompatible avec le matériel actuel $\Rightarrow$ solution à long terme.

Le protocole WPA (2/2)

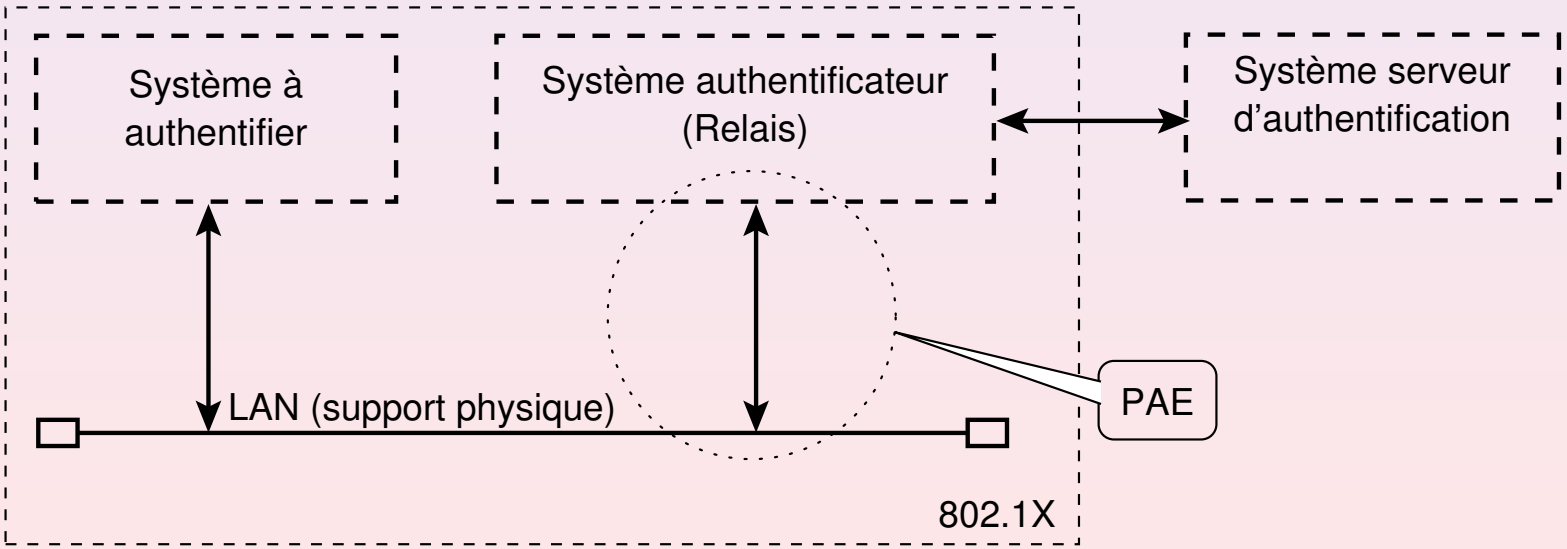
- WPA utilise le protocole 802.1X.
- Autre nom : EAP Over LAN (EAPOL).
- Permet d'authentifier les machines ou les utilisateurs connectés au réseau.
- Permet de transférer des paquets d'authentification vers différents éléments du réseau.
- Offre un mécanisme pour échanger des clés qui seront utilisées pour chiffrer les communications et en contrôler l'intégrité.
- WPA-PSK (Pre Shared Key) permet aux particuliers de bénéficier de WPA sans disposer de serveur d'authentification :
  - au début : détermination d'une clé statique ou d'une "paraphrase" (comme pour le WEP),
  - mais utilisation de TKIP,
  - ensuite : changement automatique des clés à intervalle de temps régulier.

Le protocole 802.1x

- IEEE 802.1X est un standard de l'IEEE pour le contrôle d'accès au réseau basé sur les ports.
- C'est une partie du groupe de protocoles IEEE 802 (802.1).
- Ce standard fournit une authentification aux équipements connectés à un port Ethernet.
- Il est aussi utilisé pour certains points d'accès WiFi, et il est basé sur EAP.
- 802.1X est une fonctionnalité disponible sur certains commutateurs réseau.

Les acteurs du 802.1x

- **Supplicant :** il s'agit du système à authentifier (le client).
- **Port Access Entity (PAE) :** il s'agit du point d'accès au réseau.
- **Authenticator System :** il s'agit du système authentificateur. Il contrôle les ressources disponibles via le PAE.



L'authentification

- Le système authentificateur se comporte comme un mandataire entre le système à authentifier et serveur d'authentification.
- si l'authentification réussit, le système authentificateur donne l'accès à la ressource qu'il contrôle.
- Le serveur d'authentification gère l'authentification en dialoguant avec le système à authentifier en fonction du protocole d'authentification utilisé.
- Dans la plupart des implémentations du protocole 802.1X, le système authentificateur est un équipement réseau (commutateur Ethernet, borne d'accès sans fil, ou commutateur/routeur IP).
- Le système à authentifier est un poste de travail ou un serveur.
- Le serveur d'authentification est typiquement un serveur Radius ou tout autre équipement capable de faire de l'authentification.

Le point d'accès au réseau (PAE)

- La principale innovation de 802.1X consiste à scinder le port d'accès physique au réseau en deux ports logiques qui sont connectés en parallèle sur le port physique.
- Le premier port logique est dit « contrôlé » et peut prendre deux états : « ouvert » ou « fermé ».
- Le deuxième port logique est toujours accessible mais il ne gère que les trames spécifiques au protocole 802.1X.
- Ce modèle ne fait pas intervenir la nature physique de la connexion. Il peut s'agir :
  - d'une prise RJ45 (cas du support de transmission cuivre (rien ne vaut une bonne paire de fils de cuivre)).
  - de connecteurs SC ou MT-RJ (cas de la fibre optique).
  - d'un accrochage logique au réseau (cas des supports de transmission hertzien en 802.11{a,b,g}).

Le protocole EAP

- EAP (Extensible Authentication Protocol) est un protocole conçu pour étendre les fonctions du protocole Radius à des types d'identification plus complexes.
- Il est indépendant du matériel du client Radius et négocié directement avec le supplicant (poste client, terminal d'accès).
- C'est ce qui a permis de le mettre en place rapidement sur un maximum d'appareils réseau :
  - puisqu'il n'utilise que deux attributs Radius servant de protocole de transport,
  - a conduit à une explosion de types EAP : EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MS-CHAP-V2, EAP-AKA, EAP-LEAP et EAP-FAST (Cisco), EAP-SIM, etc.

Le protocole EAP-MD5

- C'est le plus simple.
- Le client est authentifié par le serveur en utilisant un mécanisme de défi réponse :
  - Le serveur envoie une valeur aléatoire (le défi).
  - Le client concatène à ce défi le mot de passe et en calcul, en utilisant l'algorithme MD5, une valeur encryptée qu'il envoie au serveur.
  - Le serveur qui connaît le mot de passe calcule son propre cryptogramme, compare les deux et en fonction du résultat valide ou non l'authentification.
- Une écoute du trafic réseau peut dans le cas d'un mot de passe trop simple permettre de le retrouver au moyen d'une attaque par force brute basée ou par dictionnaire.

Le protocole LEAP

- Méthode propre à CISCO.
- Repose sur l'utilisation de secret partagé pour authentifier mutuellement le serveur et le client.
- Elle n'utilise aucun certificat.
- Elle est basée sur l'échange de défis et de réponses.

Le protocole EAP-TTLS

- EAP-TTLS (tunneled Transport Secure Layer).
- Il utilise TLS comme tunnel pour échanger des couples attribut valeur servant à l'authentification.
- Pratiquement n'importe quelle méthode d'authentification peut être utilisée.

Le protocole PEAP (Protected EAP)

- C'est une méthode très semblable dans ses objectifs et voisine dans la réalisation à EAP-TTLS.
- Elle est développée par Microsoft.
- Elle se sert d'un tunnel TLS pour faire circuler de l'EAP.
- On peut alors utiliser toutes les méthodes d'authentification supportées par EAP.

Le protocole EAP-TLS

- EAP-TLS : Extensible Authentication Protocol-Transport Layer Security
- C'est la plus sûre.
- Le serveur et le client possèdent chacun leur certificat qui va servir à les authentifier mutuellement.
- Cela reste relativement contraignant du fait de la nécessité de déployer une infrastructure de gestion de clés.
- TLS, la version normalisée de SSL (Secure Socket Layer), est un transport sécurisé (chiffrement, authentification mutuelle, contrôle d'intégrité).
- C'est lui qui est utilisé de façon sous-jacente par HTTPS, la version sécurisée de HTTP et pour sécuriser le Web.

Weblographie

- http://www.commentcamarche.net/authentification/radius.php3
- http://2003.jres.org/actes/paper.143.pdf
- http://raisin.u-bordeaux.fr/IMG/pdf/radius.pdf
- http://www.ysn.ru/docs/lucent/radius.pdf
- http://wifi.geeek.org/docs/ebook_sept2003.pdf
- http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques
- http://fr.wikipedia.org/wiki/Radius_(informatique)
- http://www.wifiradis.net/
- http://fr.wikipedia.org/wiki/802.1x