802.1x

La sécurité au sein d'un réseau câblé amenée par l'authentification des utilisateurs au moyen d'équipements de réseau « 802.1x » couplés à un serveur RADIUS

Diaporama Laurent PERRIN

Constatation

- Si des dispositifs existent pour sécuriser les accès depuis l'extérieur (DMZ, Pare-feux…) ou par les technologies sans-fil, force est de constater que les **prises murales** des réseaux des entreprises sont **souvent accessibles** et ouvertes, sinon au quatre vents, du moins sur des segments entiers de réseaux.

- La **technologie 802.1x** peut répondre à ces éventuels manquements à la sécurité. Elle peut apporter également plus de souplesse dans la gestion des VLAN.

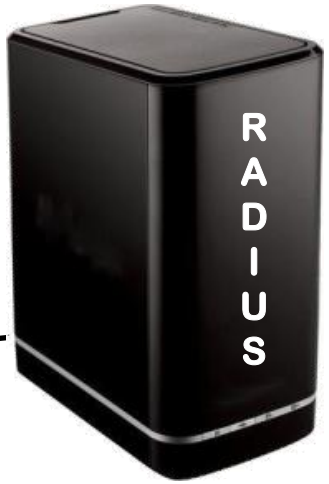
802.1x

Les acteurs en présence

Le « chef »

Équipement de réseau
relayant la demande :
Le « client RADIUS »

Le « client final »



Ordinateurs demandant
l'accès au réseau :
les « supplicants »

Le
« gardien »

Serveur acceptant
- ou refusant -
la demande :
« Serveur RADIUS »

Radius

- Remote Authentication Dial-In User Service
- Serveur qui centralise des demandes d'authentification et les soumet à un service d'annuaire LDAP ou à un service de base de données SQL.

Radius

- En premier lieu, RADIUS doit **Authentifier** les requêtes qui sont issues des clients finaux, via les clients RADIUS.
- En deuxième lieu, RADIUS a pour mission de décider quoi faire du client authentifié, et donc de lui délivrer une **Autorisation**, un "laissez-passer".
- Enfin, en bon gestionnaire, RADIUS va noter plusieurs données liées à la connexion, comme la date et l'heure, l'adresse MAC de l'adaptateur réseau du client final, le numéro de VLAN...). C'est son rôle comptable ou "d'**Accounting**".

Processus de contrôle et de gestion des accès des utilisateurs à un système informatique : **Authentication Authorization Accounting**

Les Protocoles d'Authentification

EAP **(Extensible Authentication Protocol)** est la **couche protocolaire de base de l'authentification**. Elle va servir à faire passer un **dialogue d'authentification entre le client final et le serveur RADIUS** alors que le port de connexion est fermé à toute autre forme de communication.

Les Protocoles d'Authentification

Quelles ont été - et quelles sont - ces méthodes d'authentification ?

- **Le premier protocole a été PAP (Password Authentification Protocol)**
  = Mots de passe circulaient en clair
- **Le second protocole a été CHAP (Challenge Handshake Authentication Protocol)**
  = Pas d'échange de mot de passe, principe de défis
- **Microsoft a développé une variante de CHAP appelée MS-CHAP (V1 puis V2), s'appuie sur PEAP (pas besoin de certificat sur les clients / transfert sécurisé d'info d'authentification)**
  = Ajout d'une authentification mutuelle

Principes 802.1x

Les acteurs en présence

Le « client final »

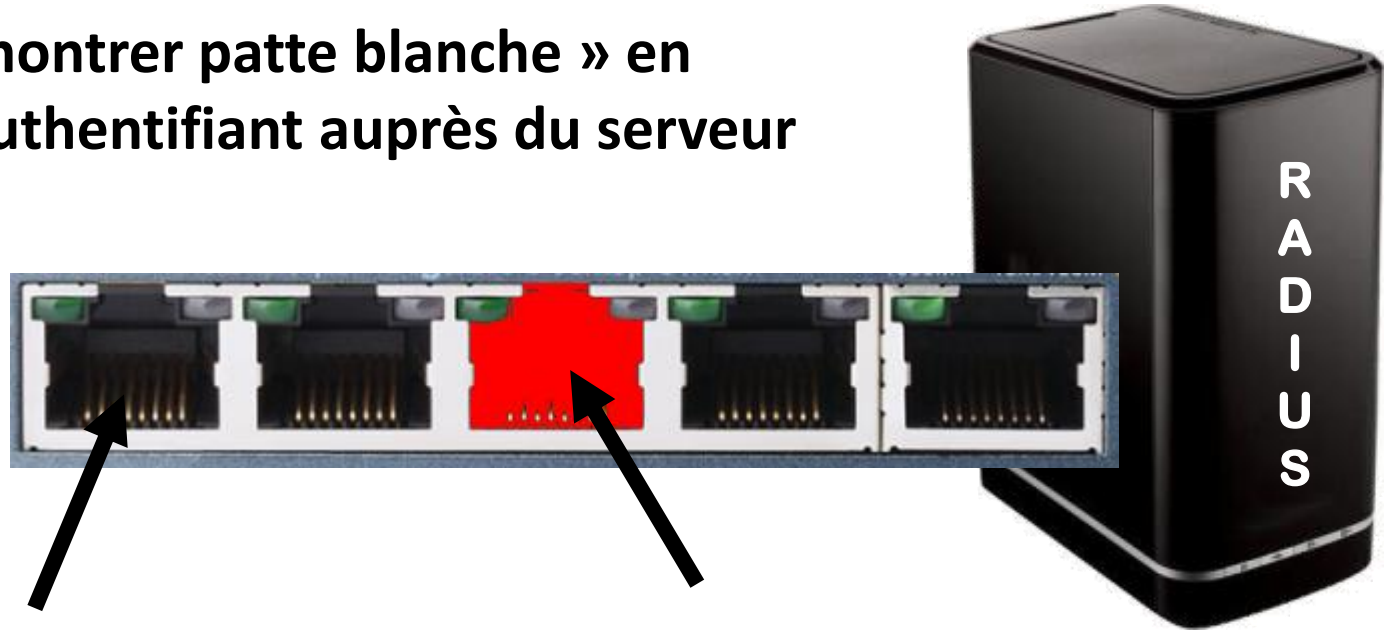
Le « gardien »

Le « chef »

LOGIN/PASSWORD

Principes 802.1x

Les ports des équipements réseaux en mode 802.1x ne sont plus en accès libre, mais il y a un préalable à leur utilisation : le client final doit « montrer patte blanche » en s'authentifiant auprès du serveur



Port N°1 en mode standard d'accès libre ouvert à tous

Port n°2 en mode « 802.1x » d'accès restreint aux clients *authentifiés*

Principes 802.1x

Comment un client peut-il s'authentifier si toute communication lui est refusée ?

➡ Grâce à l'acceptation, par le port non contrôlé des seuls paquets du protocole EAP **qui ne peut servir qu'à l'authentification**

➡ Après authentification, tous les types de paquets seront acceptés.

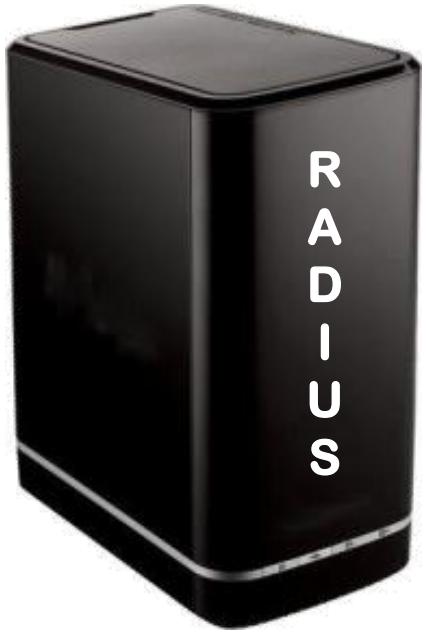
Avant authentification

Après authentification

Principes 802.1x

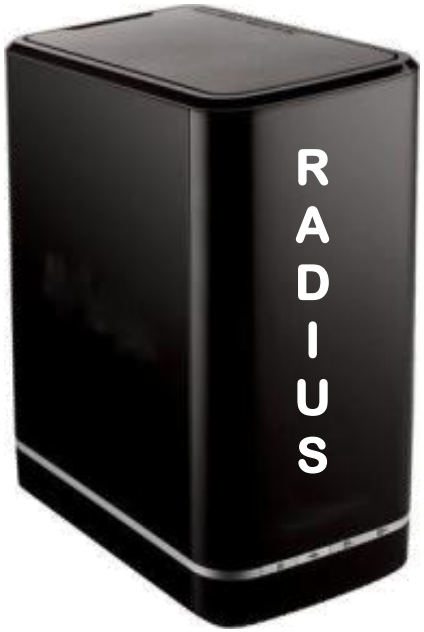
Les équipements de réseau 802.1x sont les seuls clients du serveur Radius.
Le client final ne connaît pas l'adresse du - ou des - serveurs Radius et il n'est autorisé à communiquer qu'avec l'équipement.

Échange
client/serveur



Principes 802.1x

Le serveur Radius met en œuvre les règles régissant l'acceptation ou non des demandes transmises par ses clients. Il interroge un annuaire ou une base de données SQL d'utilisateurs

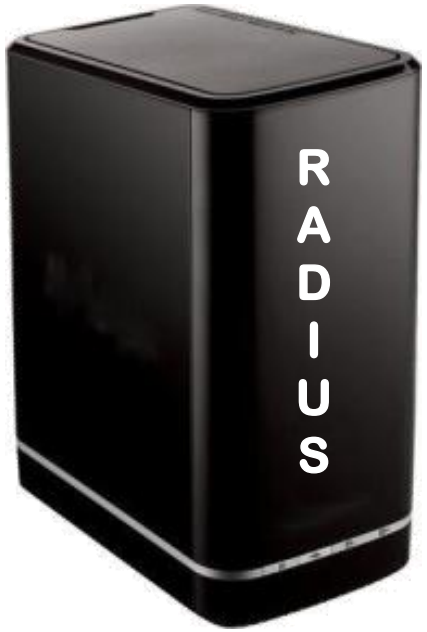


Principes 802.1x

Quelles conséquences, en cas d'acceptation ?

- autorisation d'accès pure et simple
- placement dans un VLAN dédié à l'utilisateur

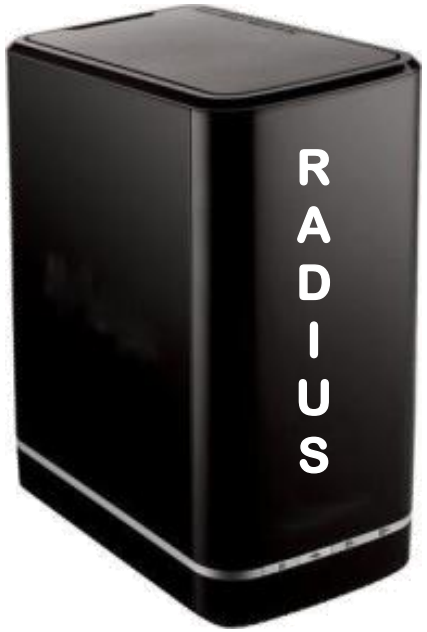
…



Principes 802.1x

Quelles conséquences, en cas de refus?

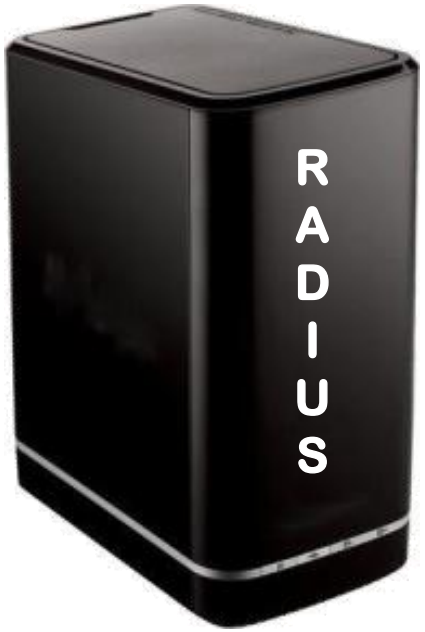
- Refus de communication pur et simple
- Placement en quarantaine (un VLAN particulier) géré par l'équipement



Principes 802.1x

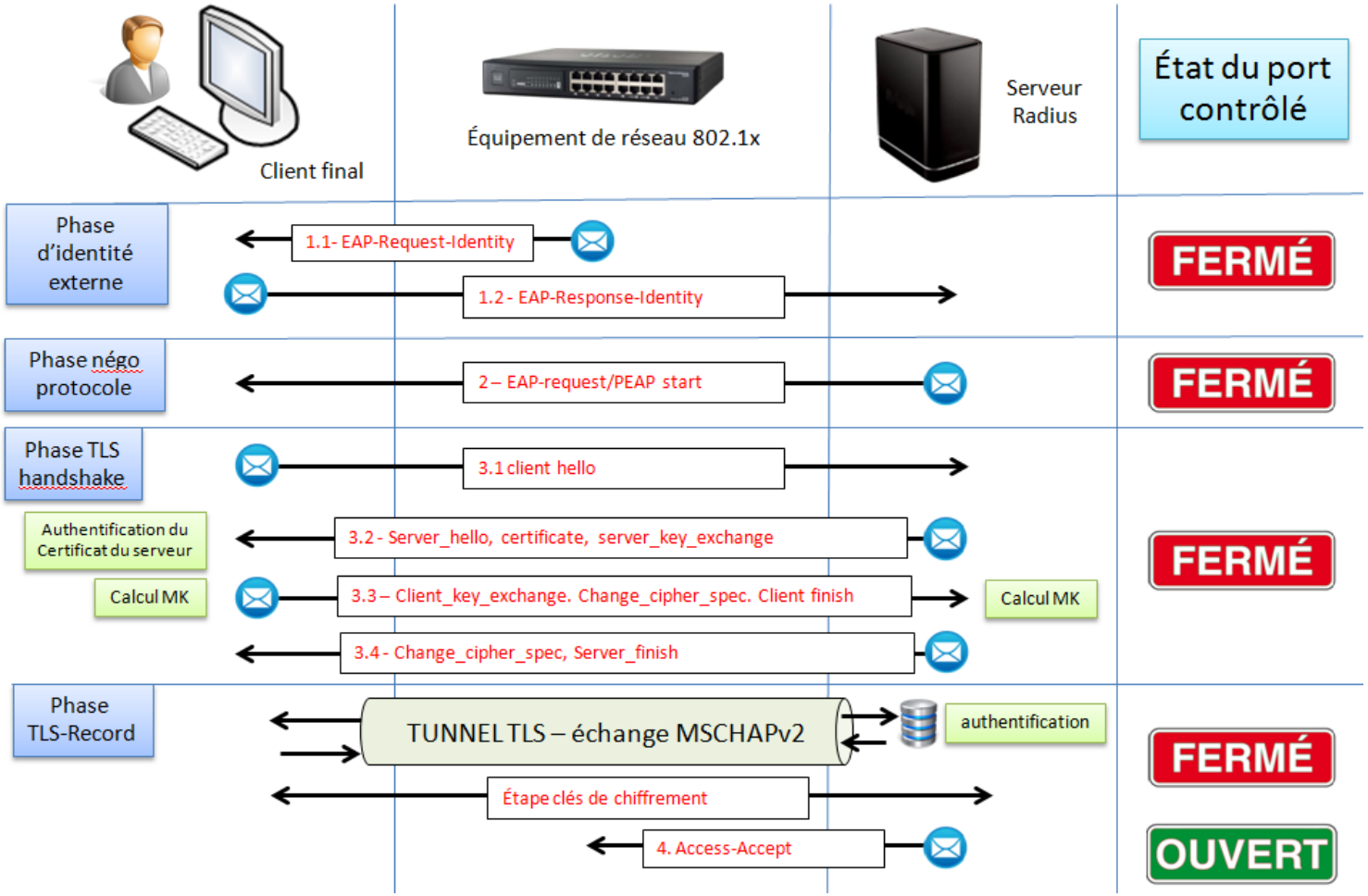
Quelles peuvent être les règles d'acceptation ?

- Utilisateur membre d'un groupe d'annuaire autorisé
- Horaire autorisé
- Adresse MAC autorisée
- « Propreté » du poste en terme d'antivirus, de mises à jour système …



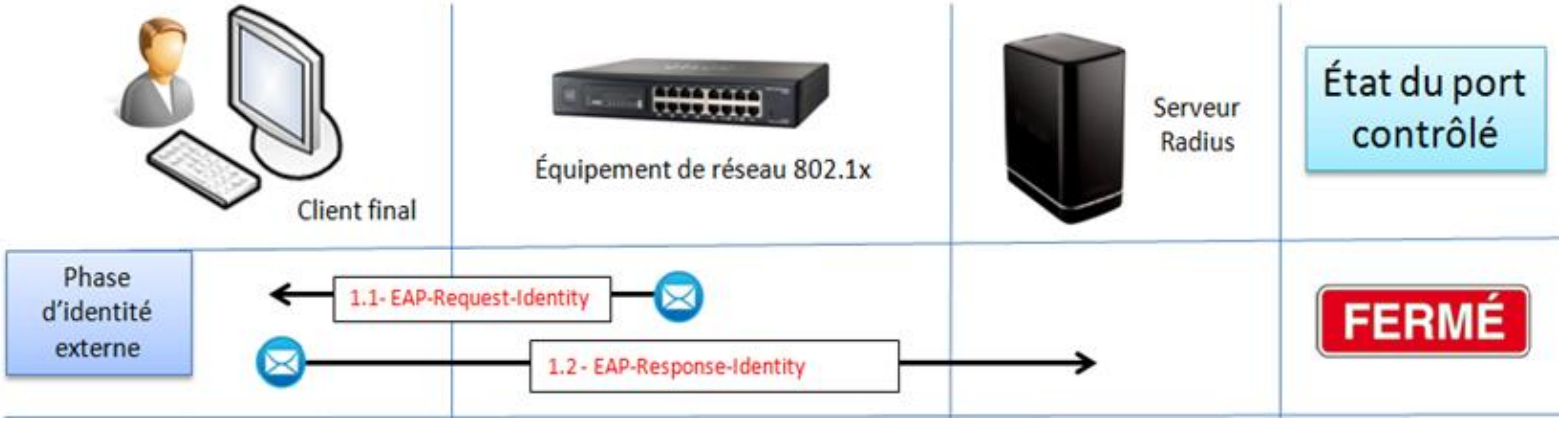
Principes 802.1x

Détails de l'Authentification RADIUS et 802.1 X (Eyrolles)



Principes 802.1x

Détails de l'Authentification RADIUS et 802.1 X (Eyrolles)
ETAPE 1 : Identité externe



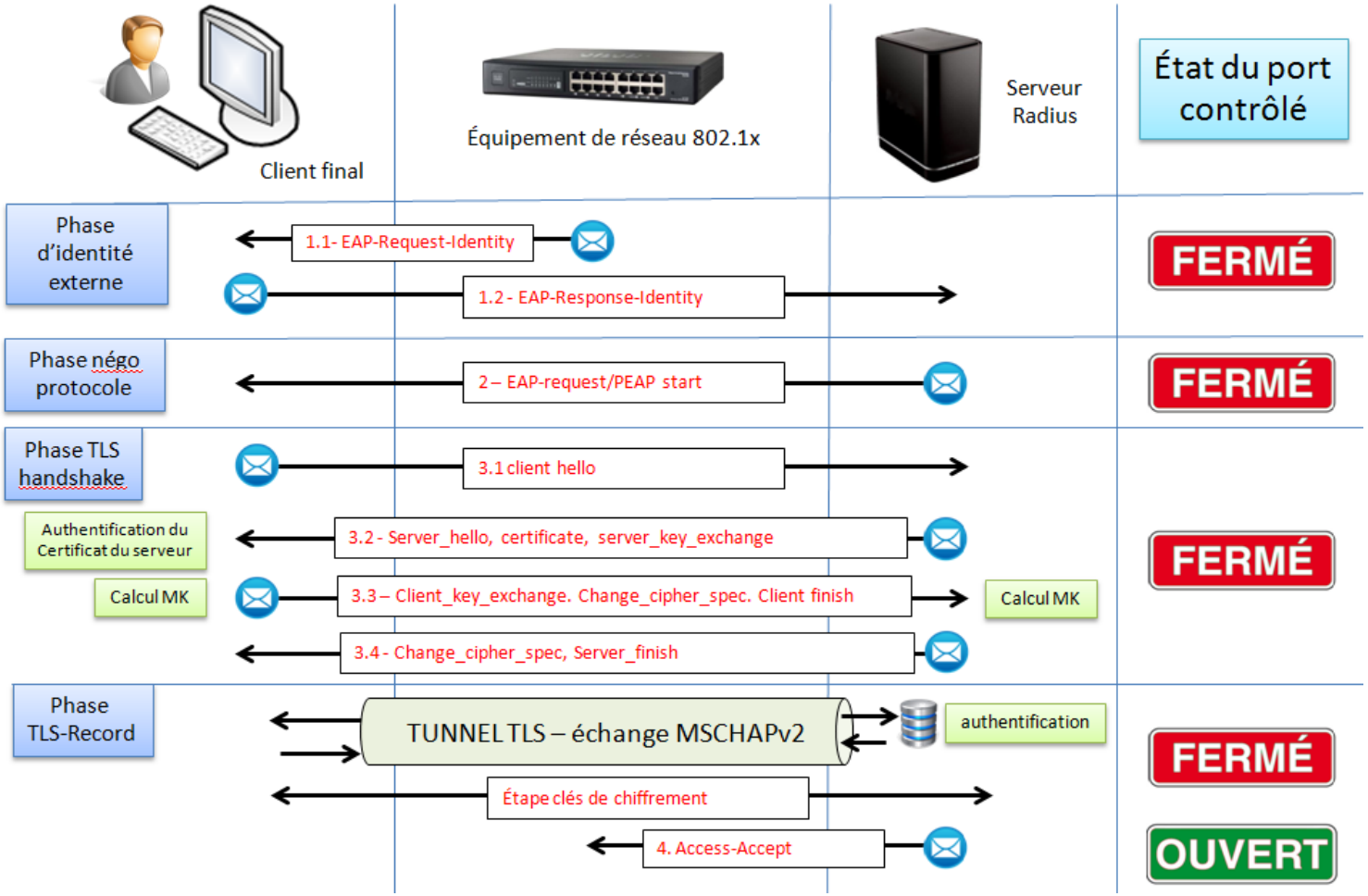
1.1 L'équipement demande au client final de décliner son identité (trame EAP-Request-Identity),

1.2 Le client répond par une trame EAP contenant son nom d'utilisateur (trame EAP-Response-Identity). Ca tombe bien, les trames EAP sont les seules autorisées à entrer dans l'équipement.

L'équipement fabrique un paquet IP [access-request] encapsulant la trame [EAP-response-Identity]. Il ajoute d'autres informations comme l'adresse MAC du client final. Ce paquet IP est envoyé au serveur RADIUS.

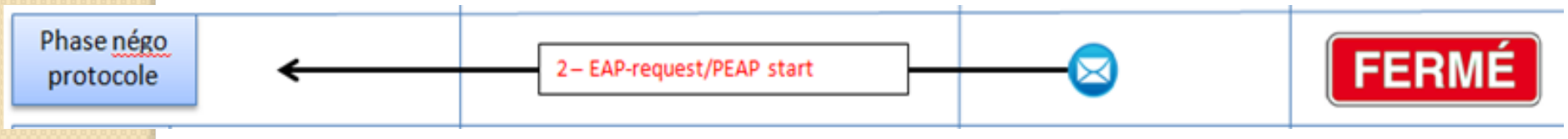
Principes 802.1x

Détails de l'Authentification RADIUS et 802.1 X (Eyrolles)



Principes 802.1x

Détails de l'Authentification RADIUS et 802.1 X (Eyrolles)
ETAPE 2 : Négociation de protocole



Le serveur RADIUS reçoit le paquet [Access-Request] et fabrique un paquet [Access-challenge] encapsulant une trame [EAP-Request] contenant une proposition de protocole d'identification, comme PEAP.

L'équipement désencapsule le paquet pour transmettre la trame EAP au client final.

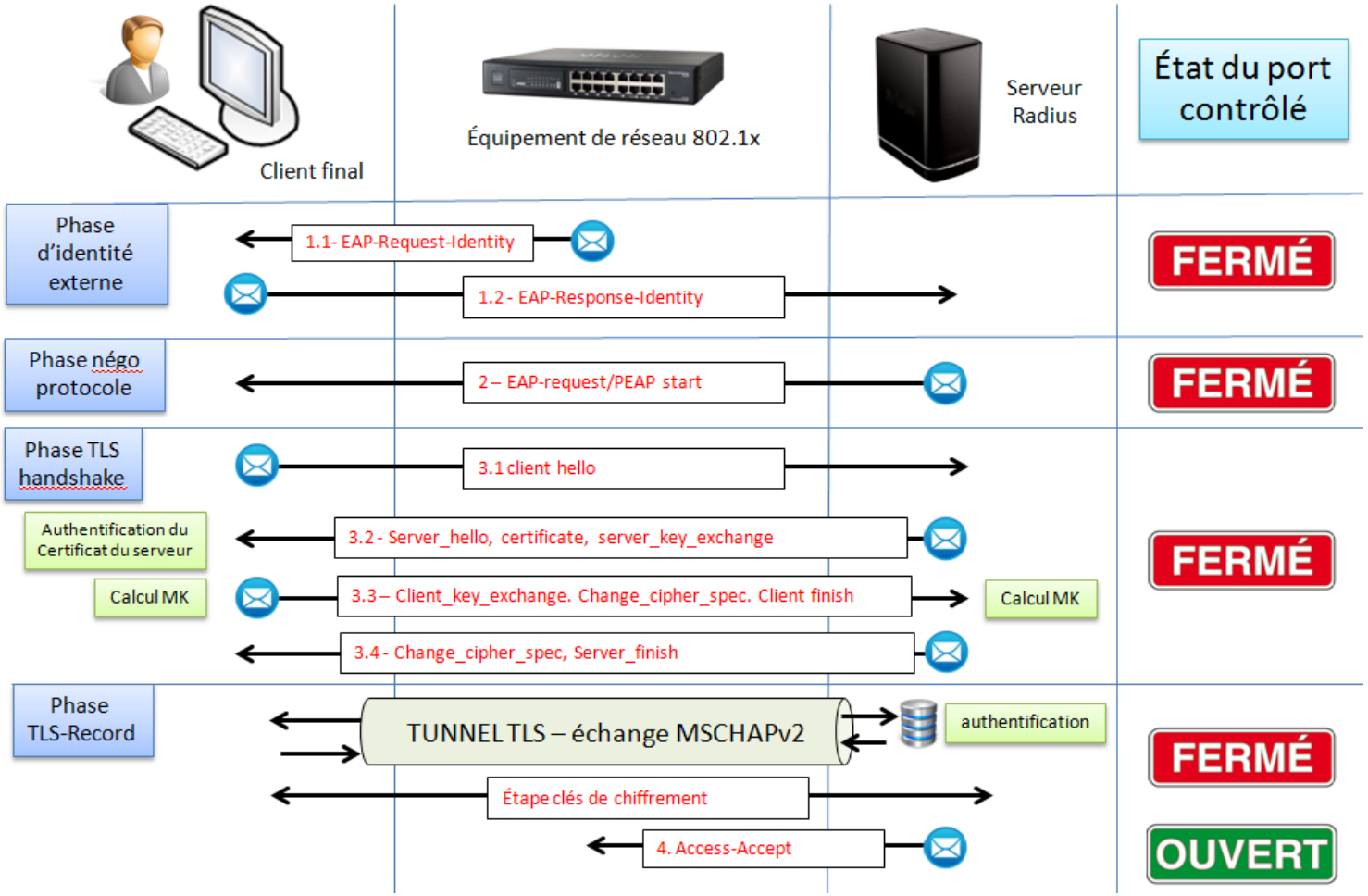
Le client final répond dans une trame [EAP-response] transmis de la même manière - indirecte par encapsulation - au serveur RADIUS.

Le client et le serveur étant tombés d'accord sur le protocole d'authentification, on passe à l'étape suivante.

Le serveur RADIUS envoie au client une requête de démarrage [PEAP-START] toujours par le mécanisme d'encapsulation d'une trame EAP.

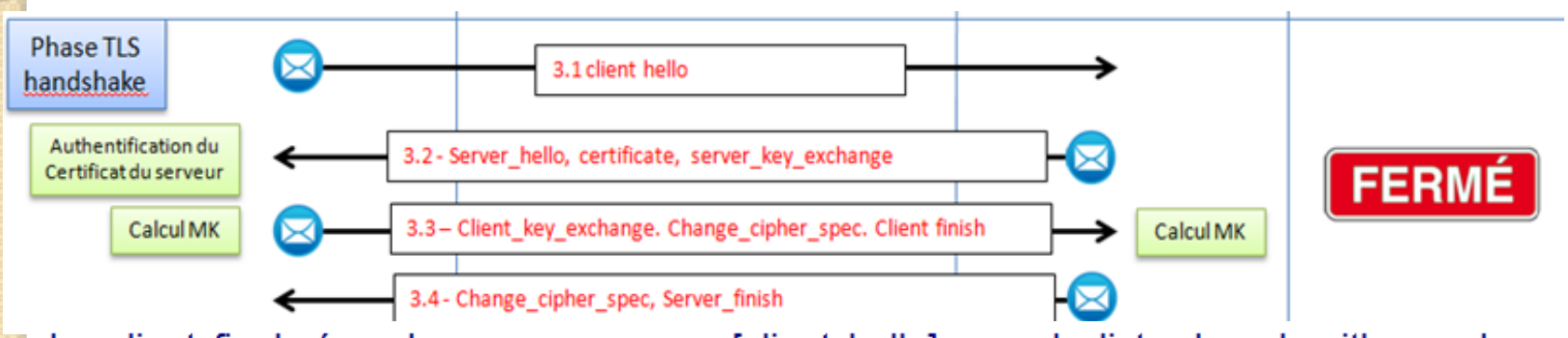
Principes 802.1x

Détails de l'Authentification RADIUS et 802.1 X (Eyrolles)



Principes 802.1x

Détails de l'Authentification RADIUS et 802.1 X (Eyrolles)
ETAPE 3 : TLS handshake (TLS remplace SSL)



Le client final répond par un message [client hello] avec la liste des algorithmes de chiffrement qu'il connait. *(3.1)*

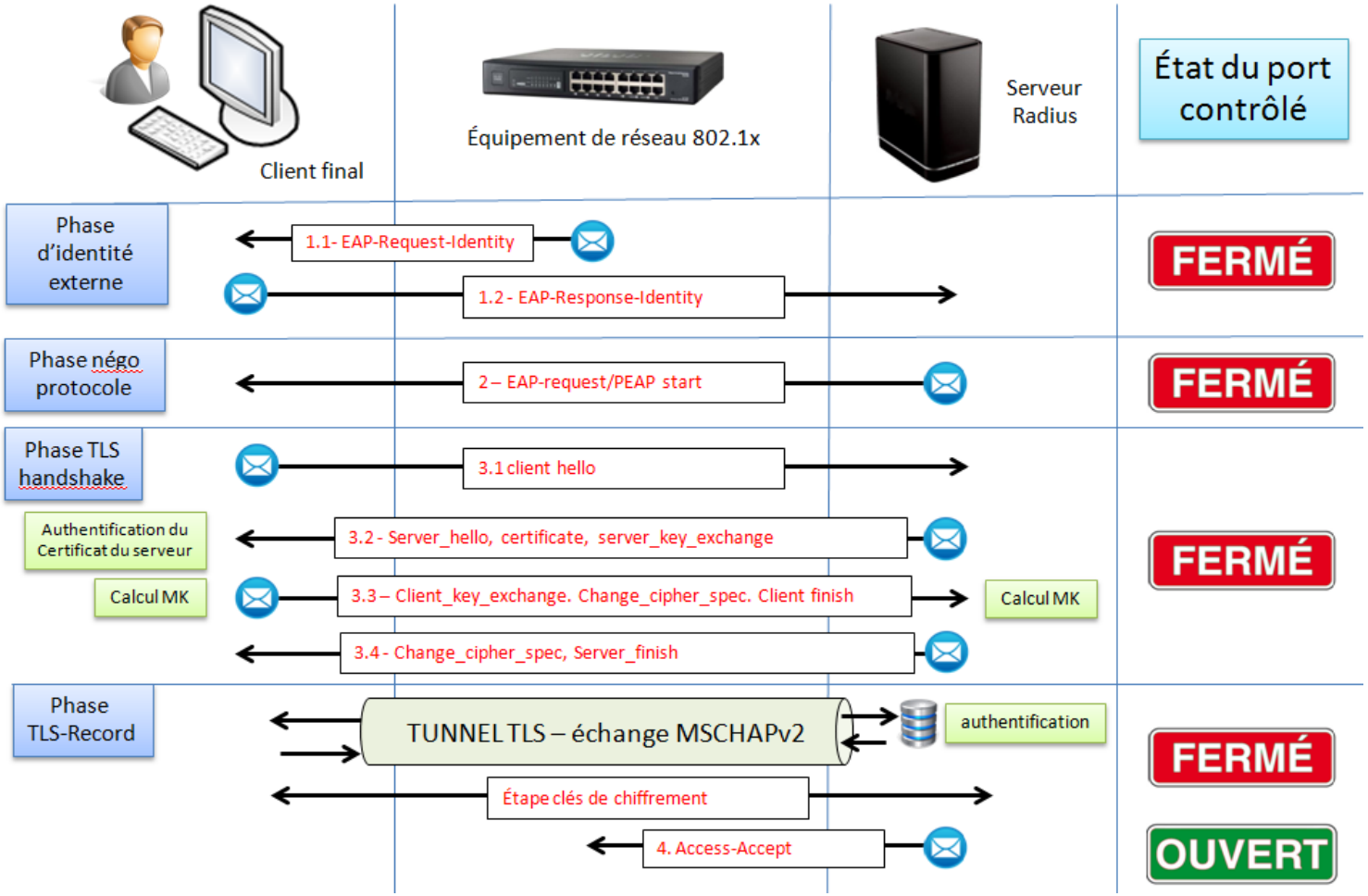
Le serveur envoie son choix d'algorithme, ainsi que son certificat et sa clé publique au client final. *(3.2)*

Le client final authentifie le serveur. Il génère une "pré-master-key" avec la clé publique du serveur *(3.3)*. Le serveur fait de même et un tunnel chiffré est établi entre eux. Le tunnel sert à protéger l'échange du mot de passe par rapport à une authentification EAP simple *(3.4)*.

Rappel : le client final n'a pas de certificat (PEAP). Attention, bien qu'on utilise TLS, on n'est pas dans "EAP-TLS", méthode utilisant des certificats serveur et client.

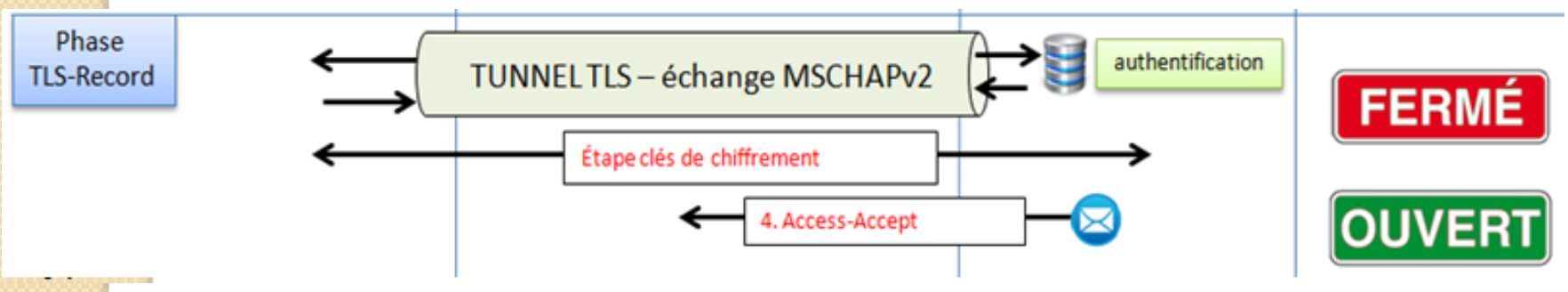
Principes 802.1x

Détails de l'Authentification RADIUS et 802.1 X (Eyrolles)



Principes 802.1x

Détails de l'Authentification RADIUS et 802.1 X (Eyrolles)
ETAPE 4 : TLS record

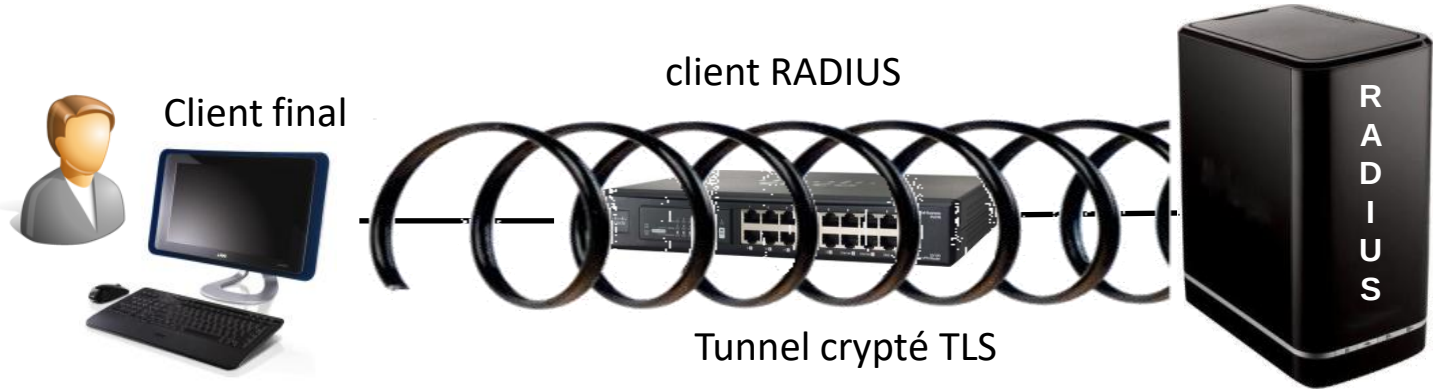


Les échanges liés au protocole de validation du mot de passe vont être effectués dans le tunnel TLS.

Le port s'ouvre lorsque le serveur envoie au client final un message [Access-Accept] après avoir vérifié le mot de passe de l'utilisateur et s'être assuré de ses autorisations.

Principes 802.1x

Articulation EAP / PEAP / MS-CHAP-V2



EAP : seul protocole de communication autorisé entre le client Radius et le client final non encore authentifié. Principe de base de 802.1X

PEAP : Protected EAP : ajout de la notion de tunnel TLS : les échanges cryptés sont transportés par EAP. Objectif : rendre invisible la nature de l'échange

MS-CHAP : méthode de reconnaissance mutuelle du client final et du serveur Radius passant par le tunnel crypté TLS.