Authentification réseau

Description du thème

Propriétés	Description
Intitulé long	Principes de la sécurisation des connexions dans un réseau câblé, par authentification de l'utilisateur. Protocole 802.1x.
Formation concernée	BTS Services Informatiques aux Organisations, parcours SISR
Matière	SISR2 - SISR5
Présentation	Ce document a pour objectif de faire découvrir les notions et techniques liées à la sécurisation des accès réseau par l'utilisation du protocole 802.1x associé à un serveur d'authentification RADIUS.
Notions	**Activités** A3.2.1 Installation et configuration d'éléments d'infrastructure A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure **Savoir-faire** Configurer les éléments d'interconnexion permettant d'établir des périmètres de sécurité. Sécuriser un service **Savoir** Normes, technologies et techniques associées à la sécurité des infrastructures réseaux
Pré-requis	Modèle OSI, VLAN, certificats
Outils	Commutateurs de niveau 2 avec prise en charge 802.1x
Mots-clés	Sécurité, Authentification, 802.1x, RADIUS, EAP, PEAP
Auteur(es)	Denis GALLOT, avec la collaboration de Daniel Régnier, Roger Sanchez et Apollonie Raffalli - relecture Gaëlle Castel.
Version	v 1.0
Date de publication	Mars 2014

Montrons Patte Blanche !

L'authentification au sein d'un réseau câblé

Protocole 802.1x Serveur RADIUS

(ou "Supplique pour être intégré dans un réseau d'entreprise")

Préambule

Ce document vise à la découverte des principes et techniques associés à l'authentification des connexions dans les réseaux câblés Ethernet. En particulier, il traitera du protocole 802.1x et des serveurs d'authentification RADIUS associés.

Si les réseaux Wifi utilisés dans les entreprises voient désormais leurs accès relativement sécurisés (par du chiffrement WPA2 par exemple) et si les accès depuis l'Internet font l'objet de technologies sécuritaires bien établies (DMZ, pare-feux, UTM ...), les prises murales sur lesquelles sont connectés les postes fixes des espaces de travail sont, dans la majorité des entreprises, "ouvertes à tous les vents" et toute personne circulant dans l'entreprise peut s'y connecter et s'introduire sur tout ou partie du réseau.

L'objectif final visé par la mise en place du couple de technologies 802.1x / RADIUS va au delà de la simple sécurisation des accès par une authentification "forte" de la personne qui cherche à se connecter sur un port réseau. Cet objectif pourra aller jusqu'à la *banalisation* de toutes les prises réseau filaires de l'entreprise. Une prise réseau quelconque ne sera plus affectée à tel ou tel VLAN. C'est à partir de l'authentification de la personne qui cherche à se connecter au réseau que l'on va déduire le périmètre de sécurité dans lequel la placer :

- Un refus pur et simple de connexion : aucun placement ;
- Le placement dans un VLAN invité ("guest") avec des prérogatives minimales, comme la simple obtention d'une adresse IP et d'un accès à Internet ;
- Le placement dans un VLAN dédié, choisi en fonction notamment du service ou du groupe auquel appartient la personne ;
- Le placement dans un VLAN à prérogatives importantes, comme un VLAN d'administration.

Il existe des technologies de filtrage sur les adresses MAC : soit circonscrites à un commutateur (doté pour chacun de ses ports, d'une liste d'adresses MAC autorisées) ou même centralisées dans un serveur RADIUS. On sait maintenant que l'adresse MAC n'est plus un élément d'authentification fiable. Pour cette raison et pour le côté malaisé de la manipulation, et surtout de la récupération des adresses MAC (particulièrement quand il s'agit de postes appartenant à des personnes extérieures à l'entreprise), on laissera ces technologies de côté dans ce document.

Sommaire

I. Principes généraux de l'authentification 802.1x

De façon imagée, l'utilisateur qui veut entrer sur le réseau va s'adresser à un "gardien" (un équipement de réseau) qui lui demande alors de décliner son identité, qui va vérifier, auprès d'un *poste de sécurité central,* que l'on peut effectivement le laisser entrer et qui prendra connaissance des prérogatives qui seront accordées à l'utilisateur après son admission.

I.1 Vocabulaire

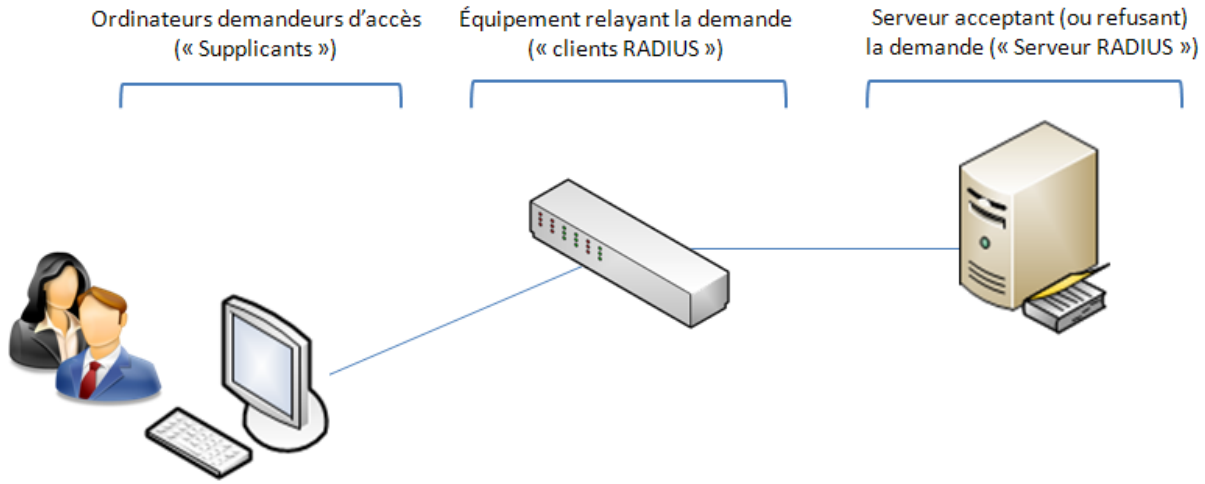


Schéma : les acteurs en présence

L'ordinateur sur lequel un utilisateur cherche à se connecter au réseau est appelé le "supplicant". Il est le "client final" de la demande de connexion. Ce peut-être avec toute forme de terminal portable, de téléphone IP ou d'ordinateur fixe. Dans la suite, nous garderons l'expression française "client final" à la place de "supplicant".

L'équipement de réseau sur lequel le client final se connecte (un commutateur - ou une borne Wifi - compatible 802.1x) relaye, en tant que *client* RADIUS, cette demande de connexion à un serveur d'authentification, le *serveur* RADIUS, qui va, par exemple, identifier la personne en rapprochant le nom de connexion et le mot de passe de ceux stockés dans un annuaire LDAP ou encore une base de données SQL.

Si l'identification réussit, l'accord est transmis au client RADIUS qui "ouvrira" alors le port de connexion.

Synonymes des termes désignant les acteurs de la connexion 802.1x :

Supplicant : on trouve aussi les expressions "client demandeur" ou "client final".

Serveur d'authentification : on parle quelquefois de serveur d'identification.

Client RADIUS : on trouve également les synonymes suivants : "Authenticator" ou NAS (Network Access Server) ou encore "contrôleur d'accès".

I.2 Le protocole 802.1x

Le protocole 802.1x est une solution standard de sécurisation de réseaux mise au point par l'IEEE en 2001. 802.1x permet d'authentifier un utilisateur souhaitant accéder à un réseau (câblé ou Wifi) grâce à un serveur central d'authentification.

L'autre nom de 802.1x est "Port-based Network Access Control" ou "User Based Access Control".

802.1x permet de sécuriser l'accès à la couche 2 (liaison de donnée) du réseau. Ainsi, tout utilisateur, qu'il soit interne ou non à l'entreprise, est dans l'obligation de s'authentifier avant de pouvoir faire quoi que soit sur le réseau. Certains équipements de réseau compatibles 802.1x peuvent réserver un traitement particulier aux utilisateurs non authentifiés, comme le placement dans un VLAN "guest", une sorte de quarantaine sans danger pour le reste du réseau.

802.1x a recours au protocole EAP (Extensible Authentification Protocol) qui constitue un support universel permettant le transport de différentes méthodes d'authentification qu'on retrouve dans les réseaux câblés ou sans-fil.

802.1x nécessite donc la présence d'un serveur d'authentification qui peut être un serveur RADIUS : un serveur Microsoft, Cisco (...) ou un produit libre comme FreeRADIUS) ou encore un serveur TACACS dans le monde fermé des équipements Cisco.

Un port d'un commutateur réglé en mode 802.1x peut se trouver dans deux états distincts :

- ✓ État "contrôlé" si l'authentification auprès du serveur RADIUS a réussi.
- ✓ État "non contrôlé" si l'authentification a échoué.

La réussite ou l'échec de l'authentification va donc *ouvrir* ou *fermer* le port à toute communication. Un port ouvert va, par exemple, permettre au client final d'obtenir une adresse IP auprès d'un serveur DHCP.

Dans des implémentations plus cloisonnées, le serveur RADIUS indiquera par exemple au client RADIUS dans quel VLAN placer le client final.

I.3 RADIUS

RADIUS (acronyme de Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des demandes d'authentification relayées par des équipements de réseau, comme des commutateurs ou bornes Wifi, considérés alors comme ses clients.

Par extension, un 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 est appelé *serveur RADIUS*.

RADIUS interroge une base de données d'authentification et d'autorisation qui peut être un domaine Active Directory, une base LDAP ou une base de données SQL. Ces bases ou annuaires peuvent se trouver sur le serveur lui-même ou sur un serveur tiers. Certaines implémentations de RADIUS disposent d'une base de données en propre.

A l'origine, RADIUS était surtout utilisé pour l'identification des clients des FAI, ses capacités de comptabilisation des accès (*accounting*) permettant notamment la journalisation des accès et leur facturation. RADIUS a été utilisé par la suite en entreprise pour l'identification des clients finals WIFI et pour l'identification des clients finals câblés.

Rôles du serveur RADIUS

En premier lieu, RADIUS doit **authentifier** les requêtes qui sont issues des clients finals, via les clients RADIUS. Cette authentification se basera soit sur un couple identifiant/mot de passe, soit sur un certificat. Cela dépendra du protocole d'authentification négocié avec le client final.

En deuxième lieu, RADIUS a pour mission de décider quoi faire du client authentifié, et donc de lui délivrer une **autorisation**, un "laissez-passer". Pour ce faire, RADIUS envoie des informations (on parle "d'attributs") aux clients RADIUS. Un exemple typique d'attribut est un numéro du VLAN dans lequel placer le client *authentifié* et *autorisé*.

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".

RADIUS est donc un serveur d'authentification, d'autorisation et de comptabilité. De façon imagée, c'est le "chef d'orchestre" des connexions 802.1X et les clients RADIUS sont ses sbires... En ce sens, il se range dans le modèle AAA (Authentication, Authorization, Accounting).

NPS (Network Policy Server) est le nom du service RADIUS des systèmes Microsoft Windows 2008 Server, en remplacement du "Service d'Authentification Internet" de Windows 2003 Server. D'autres solutions propriétaires existent, comme CISCO ACS (Access Control Server). Différentes versions libres de RADIUS existent également, comme FreeRADIUS (sous Linux ou Windows) ou OpenRADIUS (sous Linux).

RADIUS peut aussi servir à centraliser les accès sécurisés aux pages ou aux terminaux de paramétrage de tous les équipements réseau : commutateurs, routeurs, bornes wifi, contrôleurs wifi, etc.

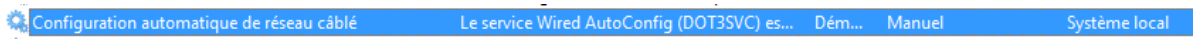
I.4 Le client RADIUS

Dans le schéma général d'une connexion 802.1x, l'élément central est l'équipement de réseau (commutateur, borne wifi, ...) désigné comme *client RADIUS*. Cet équipement doit donc être en capacité de gérer le protocole 802.1x et le protocole d'authentification EAP.

I.5 Le client final (ou supplicant)

Depuis Windows XP-SP3, les systèmes d'exploitation Microsoft disposent d'une couche "supplicante" logicielle 802.1x. Les distributions Linux disposent de paquetages comme "Xsupplicant".

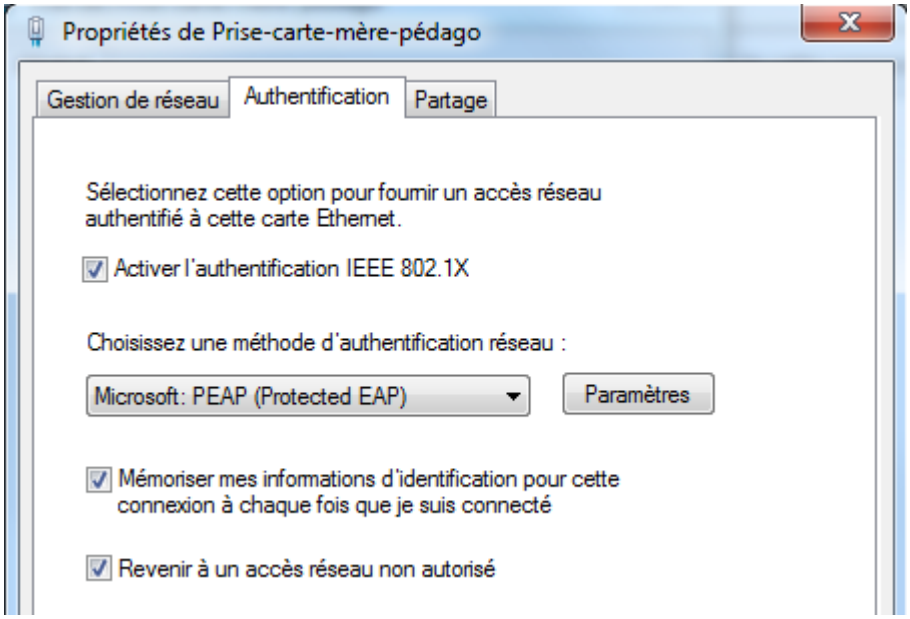
Dans Windows, pour activer cette couche logicielle, il faut lancer le service de configuration automatique de réseau câblé.



Commentaire associé à ce service:

"Le service Wired AutoConfig (DOT3SVC) est responsable de l'exécution de l'authentification IEEE 802.1X sur les interfaces Ethernet. Si votre déploiement de réseau câblé actuel applique l'authentification 802.1X, le service DOT3SVC doit être configuré de façon à s'exécuter pour l'établissement de la connectivité de Couche 2 et/ou fournir l'accès aux ressources réseau. Les réseaux câblés qui n'appliquent pas l'authentification 802.1X ne sont pas concernés par le service DOT3SVC."

La mise en route du service provoque l'apparition de l'onglet [Authentification] dans les propriétés de la carte réseau.



Signification des coches

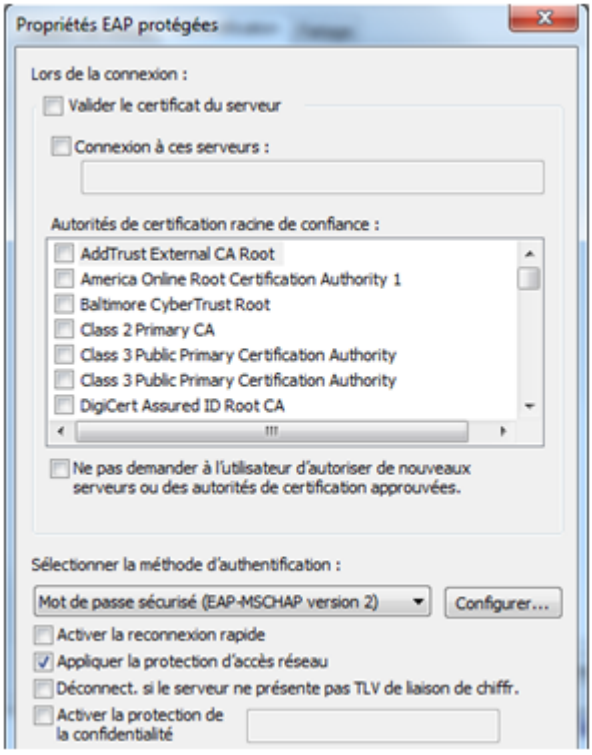
☑ "Revenir à un accès réseau non autorisé"

➔ On coche cette option si on veut que, dans le cas où le système du client final ne répondrait plus aux règles (de pare-feu, de mises à jour système, d'antivirus), sa connexion soit coupée. Ces règles d'acceptation font partie des exigences que l'on peut paramétrer dans le service RADIUS Microsoft NPS.

☑ "Mémoriser mes informations d'identification..."

➔ Mise en cache du couple identifiant/mot de passe. Cette mise en cache peut être intéressante pour une machine non intégrée dans un domaine, pour éviter de devoir se ré-authentifier. Pour nos TP, il est plus utile, pour observer ce qui se passe, de décocher cette option. Un poste intégré dans un domaine pourra utiliser les informations d'ouverture de session Windows pour l'authentification 802.1x. Ce ne sera pas demandé une seconde fois.

Ouvrons l'écran des propriétés EAP protégées en cliquant sur [Paramètres] à côté du choix [Microsoft PEAP (Protected EAP]



❑ "Valider le certificat du serveur"

➔ Cette coche n'est pas utile dans notre cas.

Dans la méthode d'authentification, on va utiliser "EAP-MSCHAP version 2" - vue plus bas).

Note : c'est par le bouton [Configurer] de l'écran ci-dessus qu'on indique si on veut utiliser - ou non - le nom et le mot de passe d'ouverture de session Windows dans le dialogue 802.1x.

Dans les phases de test, on peut relancer le mécanisme d'authentification en désactivant/réactivant la carte réseau, mais tout le dialogue ne serait pas visible dans un analyseur de trames. Il vaut mieux décocher/cocher "Activer l'authentification 802.1X" pour observer tout ce qui se passe.

I.6 Les protocoles d'authentification

EAP 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.

C'est un protocole extensible, au sens où il va permettre l'évolution de méthodes d'authentification transportées, de plus en plus sûres au cours du temps.

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

Le premier protocole a été PAP (Password Authentification Protocol) avec lequel les mots de passe circulaient en clair. La sécurité proposée par ce protocole est faible.

Le second protocole qu'ont utilisé les serveurs RADIUS a été CHAP (Challenge Handshake Authentication Protocol). Il est défini dans la RFC 1994. Avec CHAP, il n'y a pas d'échange de mots de passe sur le réseau.

Les deux interlocuteurs, qui disposent donc de la même chaîne de caractère secrète, s'authentifient sans échange du mot de passe par une technique de "challenge" (ou "défi") basée sur une fonction de hachage à sens unique du secret partagé, telle que MD5. Cette méthode était disponible avec le couple XP/Windows-2003-Server, mais ne l'est plus en génération Seven/2008.

Au début de la connexion, le serveur réclame la preuve de l'identité du client, en lui demandant de chiffrer une information. Le client ne peut relever le défi que s'il possède effectivement la clé unique et secrète partagée.

Dialogue client-serveur avec CHAP

A. Après l'établissement de la connexion, l'authentificateur envoie une valeur aléatoire xxxxxx au client.
B. Le client concatène cette valeur xxxxxx au secret partagé, applique une fonction de hachage (telle que MD5) sur la chaîne obtenue et retourne le résultat.
C. Le serveur effectue la même opération et compare avec le résultat reçu. La connexion n'est acceptée que si le résultat est identique.
D. A intervalle régulier, il y a un nouveau défi à relever pour pérenniser la connexion.

Microsoft a développé une variante de CHAP appelée MS-CHAP qui ajoute une authentification mutuelle, MSCHAP-V1, puis MSCHAP-V2.

Dialogue client-serveur avec MSCHAP-V2.

A. Le serveur envoie au client une chaîne composée d'un identifiant de session et une chaîne aléatoire xxxxx.
B. Le client renvoie son nom d'utilisateur et le résultat d'un hachage de la chaîne aléatoire xxxxx + l'identifiant de session + le mot-de-passe, et une seconde chaîne aléatoire yyyyy.
C. Le serveur vérifie le résultat (succès/échec) et retourne celui-ci, avec un hachage de la chaîne yyyyy et du mot de passe utilisateur.
D. Le client vérifie enfin la correspondance entre les chaînes.
E. La connexion est établie.

PEAP

PEAP est un protocole de transfert sécurisé (P comme "Protected") d'informations d'authentification. Il a été mis au point par Microsoft, Cisco et RSA. Il ne nécessite pas de certificat sur les postes clients, contrairement à EAP/TLS. MS-CHAP s'appuie sur PEAP.

Articulation EAP / PEAP / MSCHAP-V2

- EAP est le mécanisme permettant à un client final de pouvoir communiquer sur un port 802.1x fermé à toute autre forme de communication.
- PEAP ajoute la notion de protection des échanges par tunnel à ce mécanisme
- MSCHAP est la méthode de reconnaissance mutuelle du client serveur et du serveur RADIUS qui passe par ce tunnel.

I.7 Les différentes phases (simplifiées) d'une connexion 802.1x

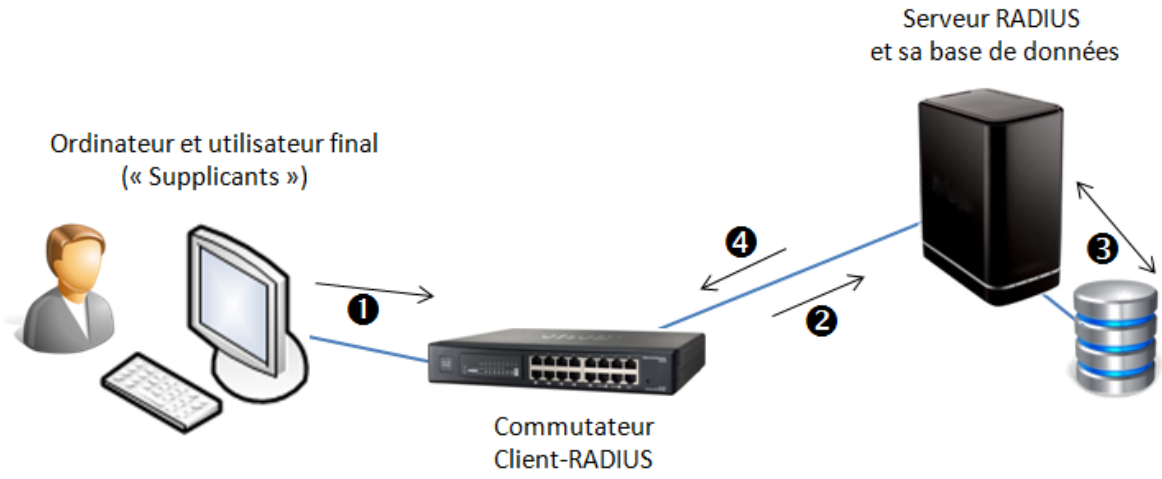
Au **démarrage** de la communication, le client final est prié d'envoyer ses identifiants au serveur RADIUS. Or, à ce moment là, le client final ne connaît pas l'adresse du - ou des - serveurs RADIUS du réseau. Il ne dispose peut-être même pas d'adresse IP. De même, le port du commutateur sur lequel il est connecté est censé être fermé (état non contrôlé).

En réalité, le port contrôlé du commutateur n'est pas totalement fermé. Il va laisser passer le protocole EAP (Phase ❶ sur le schéma suivant). Cette communication ne peut donc se faire que par des trames Ethernet de base et non par des paquets IP.

Le client final peut donc envoyer son identité dans un paquet EAP au commutateur. Celui-ci le retransmet, *encapsulé* dans un paquet au format RADIUS, au premier serveur RADIUS de sa liste (s'il en connaît plusieurs) (Phase ❷).

Le serveur RADIUS reçoit le paquet et interroge sa base de données (Phase ❸).

Il renvoie le résultat de cette interrogation au commutateur (Phase ❹), sous forme d'un commandement d'ouverture du port, éventuellement assorti d'un numéro de VLAN dans lequel placer le client final. A partir de ce moment seulement, il peut y avoir d'autres trames échangées entre le client final et le reste du réseau, comme une trame de requête DHCP par exemple.



Avant authentification

➔ Le port ne laisse passer que des trames EAP.

Après authentification

➔ Le port laisse passer tous les types de trames.

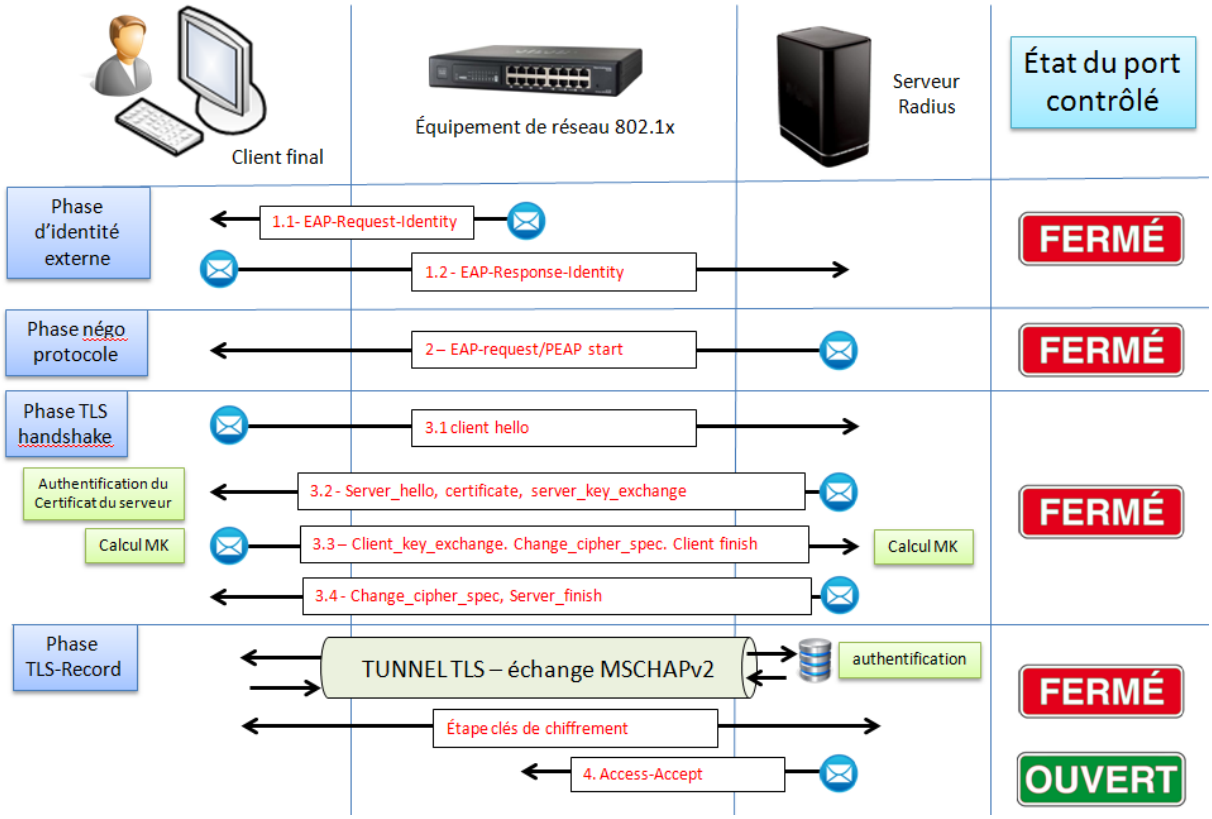
Conséquence de ce fonctionnement général.

L'équipement réseau ne connaît que le protocole RADIUS. Le protocole d'authentification entre le client final et le serveur RADIUS pourra varier sans que cela soit un blocage pour l'équipement. En ce sens, on dit que le client RADIUS est "transparent".

I.8 Et que faire des périphériques non 802.1x ?

L'objectif de contrôler toutes les prises réseau d'une entreprise en y imposant une authentification peut se heurter au fait que certains périphériques qui y sont connectés (comme des imprimantes, des vidéoprojecteurs ...) n'implémentent pas 802.1x. Il faut donc trouver d'autres solutions pour protéger ces prises : un VLAN spécifique par exemple réunissant les imprimantes, avec un serveur d'impression situé dans un autre VLAN joignable au travers d'un routeur filtrant, une protection des ports par adresse MAC, ou encore une connexion sans-fil des vidéoprojecteurs dans une technologie de cryptage comme WPA2.

II. Fonctionnement détaillé



Source : Serge Bordère - "authentification RADIUS et 802.1X", Eyrolles

Étape 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.

Étape 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 décapsule 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.

Étape 3 - TLS handshake

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

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

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

Le client final authentifie le serveur. Il génère une "pré-master-key" avec la clé publique du serveur. 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.

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.

Étape 4 - TLS record

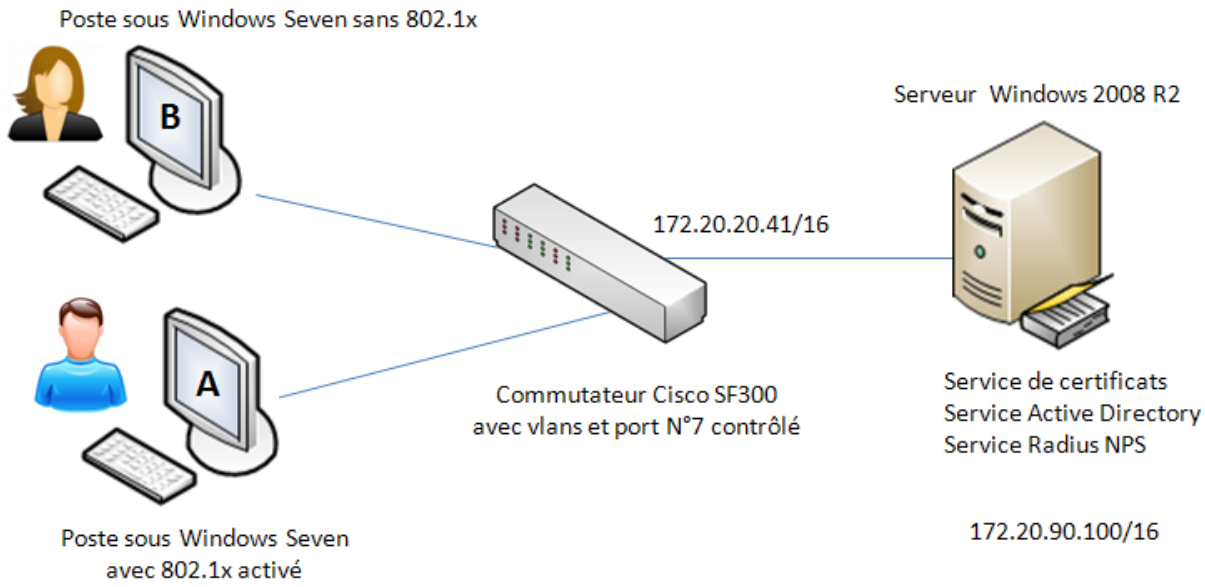
Les échanges liés au protocole de validation du mot de passe vont être effectués dans le tunnel TLS. Avec MSCHAP-V2, il s'agit des échanges vus au point I.7.

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.

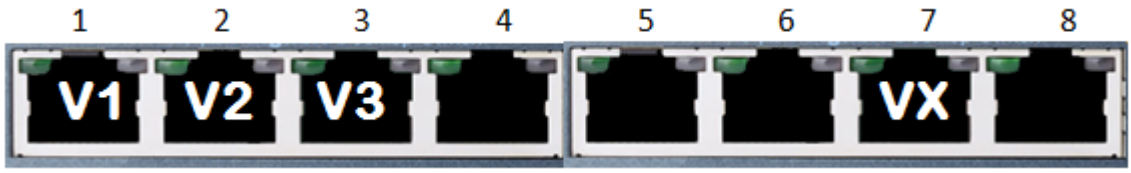
III. Un exemple d'infrastructure 802.1x

Client final : Windows Seven Pro Commutateur : Cisco SF300 - langage IOS ou interface web Serveur RADIUS NPS sur Windows Server 2008 R2

Schéma général de cette infrastructure



Les 8 premiers ports du commutateur



Le serveur RADIUS est connecté dans le VLAN 1 du commutateur, sur le port FA1 par exemple. Il héberge à la fois AD, un service de certificats et le service NPS-RADIUS.

Le client final "A" est connecté au port n°7 "contrôlé" par 802.1x du commutateur. Son VLAN dépendra de l'authentification de l'utilisateur.

Un second client final "B" pourra être connecté sur un port non contrôlé du VLAN 2 ou du VLAN 3 pour vérifier la connectivité intra VLAN 2 ou 3.

Dans un premier temps, on peut effectuer nos tests avec des IP fixes sur les postes clients. Pour mettre les clients en DHCP, il faudrait disposer d'un service DHCP dans chaque VLAN. Ceci pourrait être fait en connectant un routeur sur un port 802.1q du commutateur. Ce routeur servirait des plages DHCP dans chaque VLAN de travail et même dans le VLAN "guest".

Etapes de la mise en place

Les paramétrages à effectuer concernent le client final, le client RADIUS et le serveur RADIUS sur lequel on trouve déjà un annuaire Active Directory.

	**1.** Configurer le client final en 802.1x ▫ Service Configuration automatique de réseau câblé ▫ Onglet "Authentification" des propriétés de la carte réseau
	**2.** Paramétrer le commutateur Client RADIUS ▫ Création des VLAN ▫ Paramétrage général 802.1x - déclaration du serveur RADIUS ▫ Paramétrage des ports contrôlés 802.1x avec gestion des accès refusés (placement en VLAN "guest") ▫ Paramétrage des ports utiles non contrôlés
	**3.** Installation de deux nouveaux services sur le serveur Windows 2008 ▫ Installation d'une autorité de certification ▫ Installation du service NPS - Serveur RADIUS
	**4.** Paramétrage du service NPS ▫ Déclaration d'un client RADIUS : le commutateur ▫ Déclaration d'une stratégie de connexion ▫ Déclaration d'une stratégie d'accès réseau

Le serveur RADIUS a pour adresse IP 172.20.90.200 et communique dans le VLAN n°1 avec le commutateur Cisco qui a pour adresse IP 172.20.20.41.

III.1 Mise en place du 802.1x dans un commutateur Cisco SF-300

III.1.1 Cartographie des VLAN

- VLAN 1 : administration. Le serveur RADIUS est connecté dans le VLAN 1
- VLAN 2 et 3 : VLAN de travail pour l'affectation dynamique
- VLAN 99 : VLAN guest (quarantaine des clients non authentifiés)

III.1.2 Paramétrage et commentaires

A. Création des VLAN et déclaration du VLAN 99 en VLAN "guest"

```
MonCommutateur(config)#vlan database
MonCommutateur(config-vlan)#vlan 2
MonCommutateur(config-vlan)#vlan 3
MonCommutateur(config-vlan)#vlan 99

MonCommutateur(config)#interface vlan 99
MonCommutateur(config-vlan)#dot1x guest-vlan
MonCommutateur(config-vlan)#exit
MonCommutateur(config)#exit
```

B. Commandes générales d'activation du 802.1x et de déclaration de serveur RADIUS.

```
MonCommutateur(config)#aaa authentication dot1x default RADIUS
MonCommutateur(config)#dot1x system-auth-control
MonCommutateur(config)#RADIUS-server host 172.20.90.100
MonCommutateur(config)#RADIUS-server key Sesame9999
```

Note : le serveur RADIUS a pour adresse IP 172.20.90.100 et il est connecté dans le VLAN 1 dans lequel le commutateur a pour adresse IP 172.20.20.41.

C. Commandes 802.1x sur un port que l'on veut contrôler : fa7

```
MonCommutateur(config)#interface fa7
MonCommutateur(config_if)#dot1x host-mode multi-sessions
MonCommutateur(config_if)#dot1x RADIUS-attributes vlan
MonCommutateur(config_if)#dot1x port-control auto
MonCommutateur(config_if)#dot1x guest-vlan enable
MonCommutateur(config_if)#switchport mode access
```

Commentaires

- Le port contrôlé est placé en mode "multi-sessions" (nécessaire pour l'affectation dynamique du VLAN par RADIUS) ;
- Son ouverture sera liée à l'authentification du client final (port-control "auto") ;
- Le port est déclaré comme devant recevoir des attributs de VLAN depuis le serveur RADIUS ;
- Le port est doté de l'affectation en VLAN "guest" des clients non authentifiés ;

Note : attention, l'ordre des commandes a de l'importance.

D. Affectation des ports non 802.1x dans les VLAN de travail

```
MonCommutateur(config)#interface fa2
MonCommutateur(config_if)#switchport mode access
MonCommutateur(config_if)#switchport access vlan 2
MonCommutateur(config_if)#exit
MonCommutateur(config)#interface fa3
MonCommutateur(config_if)#switchport mode access
MonCommutateur(config_if)#switchport access vlan 3
```

III.1.3 Vérification des paramétrages

Une commande "show dot1x" est disponible avec différentes options.

Situation de départ : poste non connecté/non authentifié

```
MonCommutateur#show vlan
```

Vlan	Name	Ports	Type	Authorization
1	1	fa1,fa3-6,fa8-24,gi1-4,	Default	Required
2	2	fa2	permanent	Required
3	3		permanent	Required
99	99	fa7	permanent	Guest

▶ Le port Fa7 est dans le VLAN guest.

```
MonCommutateur#show dot1x
```

802.1x is enabled

Port	Admin Mode	Oper Mode	Reauth Control	Reauth Period	Username
fa1	Force Authorized	Authorized	Disabled	3600	n/a
fa2	Force Authorized	Authorized*	Disabled	3600	n/a
fa3	Force Authorized	Authorized*	Disabled	3600	n/a
			(...)		
fa6	Force Authorized	Authorized*	Disabled	3600	n/a
fa7	Auto	Unauthorized*	Disabled	3600	n/a
fa8	Force Authorized	Authorized*	Disabled	3600	n/a

▶ Le port Fa7 est dans en mode auto, pour l'instant interdit.

Notes sur les colonnes:

- Colonne Admin Mode : un port peut être en "autorisation forcée", en "interdiction forcée" ou en auto (accès dépendant de l'authentification 802.1x).
- Colonne Oper mode : état actuel du port → il n'est pas autorisé.
- Colonne "Reauth Control" : un "enabled" nécessiterait une réauthentification périodique du client final, la période (en secondes) étant donnée dans la colonne "Reauth period".
- Colonne Username : contiendra le nom de l'utilisateur connecté.

Messages qui sont affichés sur le commutateur lors de la connexion

Avant la demande d'authentification

```
07-feb-2013 00:10:30 %SEC-W-PORTUNAUTHORIZED: Port fa7 is unAuthorized, aggregated (1)
07-feb-2013 00:10:30 %LINK-I-Up: fa7, aggregated (1)
07-feb-2013 00:10:30 %LINK-I-Up: Vlan 99, aggregated (1)
07-feb-2013 00:10:30 %SEC-W-SUPPLICANTUNAUTHORIZED: MAC 90:2b:34:40:5f:9a was
rejected on port fa7 due to wrong user name or password in RADIUS server, aggregated (1)
```

Situation d'arrivée : authentification réussie et placement en VLAN 2

```
07-feb-2013 00:10:35 %STP-W-PORTSTATUS: fa7: STP status Forwarding, aggregated (1)
07-feb-2013 00:10:44 %LINK-I-Up: Vlan 2, aggregated (2)
07-feb-2013 00:10:44 %SEC-I-PORTAUTHORIZED: Port fa7 is Authorized, aggregated (2)
```

Résultat des mêmes commandes après la connexion de Valerie, du domaine "mars.local"

MonCommutateur#show dot1x

```
802.1x is enabled
        Admin                Oper                Reauth          Reauth Username
Port    Mode                 Mode                Control         Period
--------  -------------------  -------------  --------  ----------  -----------------
fa1     Force Authorized     Authorized     Disabled  3600        n/a
fa2     Force Authorized     Authorized*    Disabled  3600        n/a
fa3     Force Authorized     Authorized*    Disabled  3600        n/a
                                              (...)
fa7     Auto                 Authorized     Disabled  3600        valerie@mars.local
```

▶ Le port contrôlé Fa7 est dans en "oper mode" Autorisé, avec l'utilisatrice "valerie" authentifiée.

MonCommutateur#show vlan

```
Vlan    Name             Ports                      Type        Authorization
----    ----------------  -------------------------  ------------  -------------
 1      1                fa1,fa3-6,fa8-24,gi1-4,  Default     Required
 2      2                fa2,fa7                  permanent   Required
 3      3                                         permanent   Required
 99     99               fa7                      permanent   Guest
```

▶ Le port Fa7 a été placé dans le VLAN 2.

Commande show dot1x avec l'option "advanced"

MonCommutateur#show dot1x advanced

```
Guest VLAN: 99
Guest VLAN timeout:
Unauthenticated VLANs:
                                    Guest          MAC                VLAN
 Interface    Multiple Hosts        VLAN           Authentication     Assignment
-----------  --------------  --------  --------------  ----------
 fa1          Enabled         Disabled       Disabled           Disabled
                                              (...)
 fa7          Authenticate    Enabled        Disabled           Enable
```

III.2 Authentification 802.1x dans un commutateur Cisco 2960

(Mode opératoire mis au point par Daniel Régnier)

III.2.1 Mise en place de l'authentification 802.1x sur le commutateur

A - Définir un nouveau modèle d'authentification

```
(config)#aaa new-model
(config)#aaa authentication dot1x default group RADIUS
(config)#aaa authorization network default group RADIUS
(config)#dot1x system-auth-control
```

B - Définir les informations d'accès au serveur RADIUS

```
(config)#RADIUS-server host IpRADIUS auth-port 1812 acct-port 1813 key
PwdClientRADIUS
```

Exemple: (config)# RADIUS-server host 172.16.0.1 auth-port 1812 acct-port 1813 key toto

III.2.2 Configuration des ports

A - Définir l'authentification 802.1x sur un port (mode configuration d'interface)

```
(config-if)#switchport mode access
(config-if)#authentication port-control auto
(config-if)#dot1x pae authenticator
```

B - Éventuellement, affecter le port à un VLAN invité si le poste ne supporte pas le 802.1x

```
(config-if)#authentication event no-response action authorize vlan xx
```

Exemple:
(config-if)#authentication event no-response action authorize vlan 99

C - Éventuellement, affecter le port à un VLAN xx si l'authentification 802.1x a échoué

```
(config-if)#authentication event fail action authorize vlan xx
```

Exemple : (config-if)#authentication event fail action authorize vlan 100

III.2.3 Relancer l'authentification sur un port particulier

- Relancer la phase d'authentification 802.1x sur un port

```
Switch#dot1x re-authenticate interface f0/1
```

III.2.4 Afficher des informations sur l'authentification 802.1x

```
Switch#dot1x initialize interface f0/1
Switch#dot1x test eapol-capable interface f0/1
Switch#show dot1x all
Switch#show authentication interface f0/1
```

III.2 Mise en place du serveur RADIUS NPS

La mise en place du service RADIUS NPS sur un serveur Windows 2008-R2 se fait en plusieurs phases. Le serveur est un contrôleur de domaine. Il dispose donc du service Active Directory et de plusieurs utilisateurs et groupes d'utilisateurs.

Notre objectif va être d'accepter les connexions 802.1x des utilisateurs qui font partie d'un certain groupe AD et de les placer dans le VLAN 2. Une autre stratégie pourra être de placer les utilisateurs authentifiés d'un autre groupe dans le VLAN 3, etc.

Les attributs qui vont être délivrés par le serveur RADIUS en cas d'authentification sont les suivants :

- Tunnel-Type : positionné sur "VLAN"
- Tunnel-Medium-Type : positionné sur "802"
- Tunnel-Pvt-Group-ID : positionné sur le n° de VLAN de placement

La mise en œuvre de cette partie est décrite dans le document joint "installation-et-configuration-nps".

Note sur NPS

NPS permet également de mettre en place des règles d'accès réseau portant également sur la "propreté" des clients finals, en termes de mises à jour systèmes, de pare-feux, d'état de l'antivirus, etc.

▶ Ceci permet de n'accepter sur le réseau que les postes qui présenteraient des garanties de **non pollution** du reste du réseau.

IV. Pistes d'extensions de la ressource :

- Un second exemple d'infrastructure 802.1x avec un serveur FreeRADIUS
- Le paramétrage d'autres modèles de commutateurs.

Annexe

Déroulé de l'installation de NPS RADIUS et sa configuration dans fichier joint : installation-et-configuration-NPS.

LEXIQUE

AAA (Authentication Authorisation Accounting)

Label attribué aux protocoles de sécurité comportant les trois fonctions d'authentification, d'autorisation et de comptabilité.

RADIUS (Remote Authentication Dial-In User Service)

Protocole client-serveur d'authentification centralisée de terminaux ou de personnes.

TACACS (Terminal Access Controller Access-Control System)

Famille de protocoles d'authentification, d'autorisation et de comptabilité apparue dans le monde Unix. TACACS+ est la dernière version du protocole mis au point par la société CISCO.

EAP (Extensible Authentication Protocol

Protocole de base de 802.1x permettant de faire passer des informations entre le client final et le client radius *non encore authentifié* et connecté à un port à accès contrôlé par 802.1x d'un équipement de réseau.

PEAP (Protected EAP)

Extension du protocole EAP ajoutant la protection des informations qui circulent par chiffrage (tunnel chiffré).

EAPOL (EAP Over LAN)

Protocole EAP entre le poste de travail et l'équipement réseau dans un réseau filaire.

EAPOW (EAP Over WAN)

Protocole EAP entre le poste de travail et la borne Wifi pour les réseaux sans fil.

TLS (Transport Layer Security)

TLS est un protocole qui a succédé à SSL (Secure Sockets Layer), et destiné à la sécurisation des échanges par cryptage. On parle de tunnel TLS pour désigner un échange d'information indéchiffrable par un tiers.

CHAP (Challenge Handshake Authentication Protocol)

CHAP est un protocole d'authentification basé sur la résolution d'un « défi » lancé par le serveur au client. Ce défi consiste à obtenir le même résultat suite au chiffrement, chacun de son côté, d'une séquence de caractères par une clé.

MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)

Version de CHAP développée par Microsoft améliorant la sécurité par la suppression des mots de passes stockés en clair (version 1) et par l'authentification mutuelle du client et du serveur (version 2).

NPS (Network Policy Server)

Version du serveur RADIUS incluse dans les systèmes Microsoft Windows Server 2008.

ACS (Access Control Server)

Plateforme logicielle proposée par CISCO et destinée, comme RADIUS, au contrôle d'accès et à l'identification des utilisateurs.