WiFi et réseaux locaux sans fil concepts et mise en œuvre

Travaux pratiques Mise en œuvre de mécanismes de sécurité

Frédéric Weis frederic.weis@univ-rennes1.fr

Octobre 2018

Au cours de ce TP, nous allons :

- 1. Démarrer un AP Cisco, et l'intégrer à un réseau Ethernet
- 2. Créer un SSID WiFi, d'abord « caché » puis « public »
- 3. S'associer une première fois à ce SSID dans ces deux versions
- 4. Utiliser le WPA « Personal » (chiffrement TKIP ou AES + authentification par mot de passe)
- 5. Utiliser le WPA « Enterprise » (chiffrement TKIP ou AES + authentification 802.1x EAP-TLS et EAP-PEAP)

1. DEMARRAGE
2. GESTION DU SSID ET PREMIER RATTACHEMENT5
2.1. CREATION DU SSID « CACHE »
2.3. DIFFUSION DU SSID DANS LES TRAMES BALISES
<u>3. MISE EN ŒUVRE TKIP (WPA PERSONAL) SUR LE SSID V150-X8</u>
4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X
4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X 11
<u>4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X</u> 11 4.1. Un peu de theorie autour d'EAP-TLS11
 <u>4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X</u> <u>11</u> 4.1. Un peu de theorie autour d'EAP-TLS <u>11</u> 4.2. FreeRadius et openSSL
4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X
4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X
4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X 11 4.1. UN PEU DE THEORIE AUTOUR D'EAP-TLS 4.2. FREERADIUS ET OPENSSL 12 4.3. QUELQUES EXPLICATIONS SUR LE FORMAT DES CERTIFICATS 13 4.4. GENERATION DES CERTIFICATS X.509 POUR LE CLIENT WIFI ET LE SERVEUR RADIUS 13 4.5. INSTALLATION DES CERTIFICATS COTE CLIENT WIFI
4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X 11 4.1. UN PEU DE THEORIE AUTOUR D'EAP-TLS 4.2. FREERADIUS ET OPENSSL 12 4.3. QUELQUES EXPLICATIONS SUR LE FORMAT DES CERTIFICATS 13 4.4. GENERATION DES CERTIFICATS X.509 POUR LE CLIENT WIFI ET LE SERVEUR RADIUS 13 4.5. INSTALLATION DES CERTIFICATS COTE CLIENT WIFI 14 4.6. INSTALLATION DES CERTIFICATS COTE SERVEUR, ET LANCEMENT DU SERVEUR RADIUS
4. ACTIVATION DE WPA ENTERPRISE (802.1X + CHIFFREMENT TKIP) SUR LE SSID V200-X

1. Démarrage

Vous êtes connectés à un commutateur Ethernet commuté.

Chaque groupe dispose donc d'un PC Ethernet et d'un AP WiFi. Le routeur et le commutateur ont été configurés au préalable avant le démarrage du TP. Les adresses IP des AP WiFi ont été également paramétrées pour chaque groupe.

<u>Remarque 1</u> : X (1, 2, 3 ...) correspond au numéro de chaque groupe.

<u>Remarque 2</u>: Toutes les copies d'écran dans le sujet vous sont données « à titre d'exemple ». Vous devez bien entendu les adapter en fonction des paramètres que vous cherchez à configurer (utiliser les « bonnes » @IP, les « bons » numéros de VLANs etc.).

Un serveur DHCP se trouve dans le VLAN 200 et distribue des adresses dans la classe 192.168.200.X/24. Il est également capable de distribuer des adresses IP dans la classe 192.168.150.X/24 pour le VLAN 150.

Le PC (PC groupe X sur la figure suivante) dont vous disposez va exploiter une machine virtuelle Linux qui va jouer le rôle de serveur Radius pour l'authentification WiFi. La configuration de cette machine virtuelle sera abordée dans la suite du TP.

La configuration peut être résumée de la manière suivante : (pour 9 binômes)



Configurez l'interface Ethernet de votre PC en configuration automatique DHCP, puis vérifiez qu'une configuration IP vous a bien été attribuée par le serveur DHCP du VLAN 200. Vérifiez ensuite que vous accédez bien à votre AP et « au reste de l'Internet » à partir de votre PC.

Connectez-vous, depuis votre PC, au serveur WEB interne de l'AP, en utilisant l'URL <u>http://192.168.150.x/</u>, login Cisco, mdp Cisco :

Le serveur 192.168.100.11:80 requiert un nom d'utilisateur et un mot de passe. Message du serveur : level_15_access.		
Nom d'utilisateur :		
Mot de passe :		
	Annuler Se connecter	

2. Gestion du SSID et premier rattachement

2.1. Création du SSID « caché »

Définissez le SSID V150-X via l'onglet « Security -> SSID manager », en mode open, et sans chiffrement :



Ce SSID doit être lié au VLAN 150, que vous devez également définir dans l'AP (attention, la copie d'écran suivante est donnée à titre d'exemple). Notez bien qu'il s'agit d'un VLAN « natif ».

	Hostname ap			
	Security: Global SSID Manager			
	SSID Properties			
<	< NEW >	SSID: VLAN: Interface:	(V100-1] 100 ÷ Define VLANs Radio0-802.11G Glocal and 110
		Network ID:		(0-4096)
	Delete			

Descendre plus bas dans la page, et valider ces déclarations, en sélectionnant le bouton « Apply ». Attention, ce bouton est assez bas dans la page.

Multiple BSSID Beacon Settings		
Multiple BSSID Beacon		
	Set SSID as Guest Mode	
	Set Data Beacon Rate (DTIM): DIS (1-100)	Apply

Il vous reste enfin à activer l'interface radio. Via l'onglet « Network Interfaces », activez l'interface radio 802.11a ou 80211b (en fonction du modèle de l'AP). Réduisez la puissance d'émission sur l'interface (si cela est possible).

Analysez rapidement la configuration radio : sélection DFS, possibilité de gestion 802.11d, activation des différents seuils de débits ...

CISCO SYSTEMS					
	Ci	sco Aironet 1200 S	eries Access Point		
	RADIO1-802.11A STATUS	DETAILED STATUS	SETTINGS	CARRIER BUSY TEST	
EXPRESS SET-UP	Hostname ap				ap uptime is 1 hour, 19 minutes
EXPRESS SECURITY					
NETWORK MAP +	Network Interfaces: Radio1-802.11A Settin	gs			
	Enable Radio:	Enable	C Disable		
IP Address	Current Status (Software/Hardware):	Disabled 🦊	Down 🦊		
Fastlehemet Radio0-802.11G Radio1-802.11A SECURITY SERVICES + WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG	Role in Radio Network: (Fallback mode upon loss of Ethernet connection)		k to Radio Island) k to Radio Shutdown) k to Repeater)		
	Data Rates:	Best Range Best Through	put Default		
	6.0Mb/sec	Require	CEnable	C Disable	
	9.0Mb/sec	C Require	Enable	C Disable	
	12.0Mb/sec	Require	C Enable	C Disable	
	18.0Mb/sec	C Require	Enable	C Disable	
	24.0Mb/sec	Require	C Enable	C Disable	
	36.0Mb/sec	C Require	C Enable	C Disable	
	48.0Mb/sec	C Require	Enable	C Disable	
1	54.0Mb/sec	C Require	Enable	C Disable	

Par exemple, pour « lever » l'interface 802.11a, on sélectionne l'option **NETWORK INTERFACES** du menu gauche. Puis sélectionnez **Radio1-802.11A**, puis l'onglet **SETTINGS**, et sélectionner finalement l'option **Enable**, et le bouton **Apply** se trouvant plus bas dans la page (l'activation de l'interface peut prendre un peu de temps).

	RADIO1-802.11A STATUS		DETAILED STATUS		CARRIER BUSY TEST
HOME	Hostname ap			-	L
EXPRESS SET-UP					
EXPRESS SECURITY					
NETWORK MAP +	Network Interfaces: Radio1-802	2.11A Settin	gs		
NETWORK INTERFACES	Enable Radio:	<	• Enable	O Disable	
IP Address	Current Status (Software/Hard	ware):	Disabled 🦊	Down 🦊	
FastEthernet Radio1-802.11A SECURITY + SERVICES + WIRELESS SERVICES + SYSTEM SOFTWARE + EVENTLOG +	Role in Radio Network:		Access Point Access Point Access Point (Fallback t Access Point (Fallback t Repeater Root Bridge Non-Root Bridge Non-Root Bridge with Wireles Non-Root Bridge with Wireles	o Radio Shutdown) o Repeater) s Clients reless Clients	
			Workgroup Bridge		
			OScanner		
	Data Rates:	6.0Mb/sec	Best Range Best Through	Default Cefault	O Disable
	HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP + ASSOCIATION + NETWORK IVERFACES Paddress FastEthernet Radio1-802.110 Radio1-802.110 Radio1-802.110 Radio1-802.110 SERVICES + SYSTEM SOFTWARE + EVENT LOG +	HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP NETWORK MAP * NETWORK FastEthernet Radio-802.110 Radio1-802.110 FastEthernet Radio-802.110 Radio1-802.110 * Radio1-802.110 * Radio-802.110 Radio Network: * SERVICES * SYSTEM SOFTWARE * EVENT LOG *	HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP * MORE IP Address FastEthernet Radio1-802.11A Radio1-802.11A SERVICES * SYSTEM SOFTWARE EVENT LOG * Data Rates: 6.0Mb/sec	HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP + ASSOCIATION NETWORK MAP + ASSOCIATION NETWORK MAP - RADIO1-802.11A Status Bastelhemet Radiol-802.11A FastElhemet Radiol-802.11A GECUBITY + SYSTEM SOFTWARE EVENT LOG + EVENT LOG Data Rates: Best Range Best Through 6.0Mb/sec	HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP + ASSOCIATION NETWORK MAP * ASSOCIATION * Retrogeneration * Radiol-802.11A Settings * Settings * Current Status (Software/Hardware): Disable Current Status (Software/Hardware): PastEthernet Radiol-802.11A ************************************

2.2. Attachement au SSID

Le SSID V150-X est « caché ». Il est donc nécessaire de le déclarer dans les réseaux favoris de votre station mobile à la première connexion. Par exemple, sur une station Windows, vous pouvez le faire par exemple via l'option « Propriétés » sur votre interface WiFi (accessible via un « clic bouton droit » sur cette interface WiFi) :

Utiliser Windows pour c	onfigurer mon réseau sans <u>fi</u> l	
<u>deseaux disponibles :</u> Pour vous connecter, vous déconnecter ou trouver plus d'informations à propos des réseaux sans fil à portée, cliquez sur le bouton ci-dessous.		
	Afficher les réseaux sans fil	
Se connecter automatiqu	Jement aux réseaux disponibles dans	
Se connecter automatiqu l'ordre indiqué ci-dessous	Jement aux réseaux disponibles dans s : <u>Monter</u> <u>Descendre</u>	

Notez que vous devez déclarer que le SSID peut être accroché « même s'il est caché ». Votre carte WiFi va lancer une série de trames 802.11 « probe request » sur toutes les bandes de fréquence qu'elle supporte, en recherchant le SSID V150-X (qui est dans votre cas son unique réseau favori).

Depuis votre terminal WiFi (Windows, MAC OS, Iphone, Android etc.), vérifiez alors que la connexion est active, et que le serveur DHCP vous a délivré une configuration WiFi dans le VLAN 150 (plage d'@ IP 192.168.150.X/24).

2.3. Diffusion du SSID dans les trames balises

Supprimez le SSID V150-X de vos réseaux favoris à partir des propriétés de votre carte WiFi (« oubliez » le réseau WiFi).

Nous allons maintenant déclarer le SSID comme « public ». Autrement dit, on va le diffuser dans les trames *beacon* de l'AP, afin de le rendre automatiquement visible par les clients WiFi. Pour ce faire, procédez comme suit (options se trouvant tout en bas de la page Web) :

Guest Mode/Infrastructure SSID Sett	ings	
Radio0-802.11G: Set Beacon Mode:	Single BSSID Set Single Guest Mode SSID: <u> </u>	
Set Infrastructure SSID:	Multiple BSSID KNONE > Force Infrastructure Devices to associate only to this SSID KNONE >	
Radio1-802.11A: Set Beacon Mode:	Single BSSID Set Single Guest Mode SSID: V200-1 : Multiple BSSID	
Set Infrastructure SSID:	<none> 1 Force infrastructure Devices to associate only to this SSID</none>	Apply Cancel

Sans passer par les propriétés de votre carte WiFi, le SSID doit être cette fois-ci visible automatiquement par votre PC. Votre carte va tout simplement scanner l'ensemble des bandes de fréquence qu'elle supporte, et rend visible à l'utilisateur l'ensemble des SSID publics. Cliquez sur le SSID V150-X, et vérifiez que vous l'accrocher correctement.

3. Mise en œuvre TKIP (WPA personal) sur le SSID V150-X

Nous allons protéger l'accès au SSID V150-X par un mot de passe. Ce dernier sert également à chiffrer la liaison sans fil. C'est de type de protection que vous utilisez sur la *box* de votre domicile.

Hostname ap				ap uptime is 12 minutes
Security: Encryption Manager				
Set Encryption Mode and Keys for V	LAN:		100 ‡	Define VLANs
Encryption Modes				
O None				
O WEP Encryption	Optional	Cisco Compliant TH	KIP Features: 🔄 Enable Message Integrity Check (MIC)	
• Cipher	ТКІР		Enable Per Packet Keying (PPK)	
Encryption Keys				
		Transmit Key	Encryption Key (Hexadecimal)	Key Size
	Encryption Key 1:	0		128 bit ‡
	Encryption Key 2:	۲		128 bit ‡
	Encryption Key 3:	0		128 bit ÷
	Encryption Key 4:	\bigcirc		128 bit ÷

Via l'onglet « SECURITY -> Encryption Manager » :

Puis revenir à la configuration de votre SSID à ce niveau :

Client Authenticated Key Management			
Key Management:	Mandatory 🗧	ССКМ	🗹 WPA
WPA Pre-shared Key:		• ASCII (Hexadecimal

Le mot de passe sélectionné doit comporter au moins 8 caractères, par exemple tpsecret.



client, vous devez maintenant vous attacher au SSID via WiFi. Un conseil : supprimez le SSID de vos propriétés réseaux sous Windows, et reconnectez-vous. Cela impose à votre ordinateur de « renégocier » les paramètres de sécurité imposés par l'AP.

Comment validez-vous votre configuration ?

4. Activation de WPA enterprise (802.1x + chiffrement TKIP) sur le SSID V200-X

Dans ce chapitre, nous allons mettre en œuvre chiffrement TKIP + authentification 802.1x, EAP-TLS dans un premier temps, puis EAP-PEAP dans une deuxième étape.

4.1. Un peu de théorie autour d'EAP-TLS

Tout comme le protocole https, EAP-TLS s'appuie sur le protocole TLS pour gérer les mécanismes d'authentification. Cette méthode utilise des **certificats électroniques X.509** côté client 802.11 et côté serveur Radius. Un certificat est un document électronique contenant un certain nombre d'information (nom du propriétaire, période de validité, clef public du certificat, signature numérique (empreinte via hashage + cryptage) du certificat ...). Ces informations vont être utilisées par une personne pour prouver son identité.

Plus précisément, on s'appuie sur une autorité de certification (CA). Une autorité de certification est une organisation qui délivre des certificats électroniques à une population. Un CA possède lui-même un certificat (le plus souvent « autosigné », c'est à dire qu'il a généré lui-même), et utilise ce certificat « racine » pour créer les certificats qu'il délivre ensuite.

Une personne se voit donc délivrer un certificat par le CA, qu'elle installe localement. Ce certificat lui permettra de prouver son identité à une entité distante, à condition que cette même entité « fasse confiance » à ce CA. Pour cela, il faut installer localement le certificat « racine » du CA, et déclarer ce certificat comme étant « de confiance ». Et c'est ce couple certificat de la personne + certificat racine du CA « de confiance » qui va permettre de valider le fait que **le certificat reçu a bien été émis par un CA « de confiance »**.

Pour réaliser cette partie, nous avons donc besoin :

- 1. D'un client supportant EAP-TLS et les certificats X.509
- 2. D'un serveur Radius supportant EAP-TLS et les certificats X.509
- 3. D'une autorité de certification (CA) pour générer les certificats X.509 racine, client et serveur

Dans cette partie du TP, nous allons :

- 1. Générer un certificat « racine » pour le CA
- 2. Générer des certificats pour le client 802.11 et le serveur Radius
- 3. Installer les deux certificats (équipement + racine) au niveau du client 802.11 et du serveur Radius
- 4. Configurer l'AP pour relayer les données EAP vers le serveur Radius
- 5. Lancer le serveur Radius, et valider le processus d'authentification

Ainsi, via EAP-TLS, chaque partie possède un certificat pour prouver son identité. L'avantage de cette méthode est qu'elle est très sécurisée, les certificats étant échangés via un tunnel crypté. Son principal inconvénient est qu'elle est lourde à mettre en œuvre, notamment au niveau de la gestion des certificats (création, suppression, révocation, distribution ...). Tous ces mécanismes reposent sur une « infrastructure de gestion des clefs » (PKI : Public Key Infrastructure), complexe à déployer et à maintenir.

4.2. FreeRadius et openSSL

FreeRadius est une implémentation d'un serveur Radius, sous licence GPL, fonctionnant sur la plupart des Unix. Le code source est disponible sur <u>http://www.freeradius.org</u>. FreeRadius supporte la plupart des mécanismes d'authentification EAP, notamment EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP ... Pour gérer EAP-TLS, EAP-TTLS et EAP-PEAP, freeRadius a besoin des fonctions offertes par le protocole TLS. Il fait donc appel à un programme externe : openSSL (<u>http://www.openssl.org</u>). OpenSSL est un ensemble de bibliothèques écrit en C, offrant une implémentation des protocoles SSL/TLS, ainsi que des fonctions de manipulation des certificats X.509.

Dans le cadre de ce TP, openSSL sera utilisé

- 1. Par freeRadius, pour réaliser les appels EAP-TLS
- 2. Comme autorité de certification pour créer les certificats X.509

Ces deux logiciels vont sont fournis via une machine virtuelle installé sur votre PC. Lancez VirtualBox.

Vous devez ensuite respecter les étapes suivantes :

- Avant de démarrer cette image, assurez-vous que la configuration de l'interface réseau est correcte : 1^{ac} interface de votre PC en mode pont, ce qui vous permettra de disposer d'un serveur accessible comme le serait un OS serveur natif.
- Démarrez la VM.
- Connectez vous: user + bonjour, puis sudo su, mot de passe bonjour

Attention, utilisez la commande halt si vous souhaitez arrêter cette machine Linux.

- Editez le fichier /etc/network/interfaces (utilisez nano si vous êtes allergique à l'éditeur vi) et validez votre configuration IP : 192.168.200.X/24, routeur par défaut 192.168.200.253.
- Redémarrez votre interface réseau : /etc/init.d/networking restart

- Configurez votre serveur DNS dans le fichier /etc/resolv.conf, ligne nameserver, avec l'adresse 192.168.100.1.
- Vérifiez finalement la connectivité vers Internet : ping <u>www.google.fr</u>

4.3. Quelques explications sur le format des certificats

Les certificats X509 peuvent être encodés suivants deux formats : DER et PEM. Le format DER correspond à un certificat encodé en **binaire**, alors que le PEM correspond à un format ASCII éditable. Le format à utiliser (binaire ou ASCII) dépend du logiciel exploitant le certificat. A noter qu'il est possible d'utiliser DER et PEM comme extension pour les certificats.

Il existe des extensions particulières pour désigner les certificats :

- .p12 désigne les certificats PKCS#12. Le certificat contient la clé privée du destinataire du certificat ainsi que le certificat associé. Il peut contenir éventuellement le certificat de l'autorité racine (ce n'est pas le cas dans ce TP).
- .crt et .cert sont des extensions utilisées pour désigner un certificat et peuvent être exigées par certains systèmes d'exploitation. Le certificat peut être encodé au format PEM ou DER.

4.4. Génération des certificats X.509 pour le client WiFi et le serveur Radius

Il s'agit ici de reproduire ici quelques mécanismes propres à une PKI. Vous allez générer trois certificats : un pour le client, un pour le serveur Radius, et un certificat racine qui va permettre au client et au serveur de « déclarer » leur confiance à votre autorité de certification.

La manipulation des commandes offertes par openSSL pour créer des certificats X.509 est complexe. Nous utilisons trois scripts de génération : **CA.root**, **CA.clt et CA.svr** installé dans le répertoire /etc/certgen.

Chaque script produit trois certificats : .p12, .pem et .der.

Ces trois commandes exécutées **sans paramètre** vous indiquent en retour quels sont les paramètres attendus en entrée. Commencez par en prendre connaissance.

Vous devez utilisez des mots de passe différents pour protéger les clés privées des différents certificats, par exemple :

- Clé privée de l'AC protégée par « secretAC »
- Clé privée du client protégée par « secretclient »
- Clé privée du serveur protégée par « secretserver »

A noter que les scripts exécutés créent un résumé dans le fichier RESUME dans /etc/certgen.

Ces trois scripts s'appuient par défaut sur les informations du fichier « openssl.cnf » : nom de l'utilisateur, @mail, nom de l'organisation ... Toutes ces informations seront ensuite utilisées pour renseigner les attributs des certificats. Ces scripts sont exécutés à titre d'exemple, dans le cadre de notre autorité de certification. Bien entendu, si on cherche à mettre en œuvre une

véritable PKI, les commandes openSSL peuvent être utilisées en conjonction avec d'autres langages (Php, perl ...) et des environnements Web permettant d'assurer la distribution des certificats.

Une fois certificats les créés, la commande ./INSTALL-client nom du certificat client installe les certificats pour le client (CA+client) dans le répertoire du serveur FTP (/home/ftp) de VM. La commande votre nom du certificat serveur ./INSTALL-serveur installe les certificats (CA+serveur) dans le répertoire /etc/freeradius/certs du serveur Radius.

Vous devez effectuer les opérations suivantes (en les analysant pour bien les comprendre) :

- Placez vous dans le répertoire /etc/certgen.
- Supprimer d'anciens certificats dans ce répertoire via la commande . / PURGE.
- Créez un certificat serveur de nom server et d'identité server.
- Créez un certificat client de nom client et d'identité usermobile.
- Installez les certificats pour l'export FTP et le la configuration du serveur Radius.

4.5. Installation des certificats côté client WiFi

L'exemple d'installation vous est donné ici pour une station Windows. Il peut tout à fait être appliqué sur un Mac, un PC Linux ou sur un Smartphone Android ou Iphone.

Deux fichiers générés par les scripts précédents sont nécessaires côté client Windows ou MAC : **root.der** (certificat du CA), et **client.p12** (fichier contenant les informations nécessaires pour installer le certificat du client). Sous Linux, il faut utiliser les fichiers **root.pem** et **client.p12**, alors qu'Android demande les fichiers root.crt (au format DER) et client.p12.

En théorie, ces fichiers doivent être transmis via un canal sûr sur le disque du client : tunnel chiffré, clef USB ... Ici, vous pouvez les récupérer via le protocole ftp, et le compte anonymous (un ftp public sans mot de passe). Ainsi, lancez une connexion vers l'URL *ftp://@IP de votre serveur* depuis le navigateur de votre PC.

Une fois ces deux fichiers récupérés, cliquez sur le certificat du CA :





Vous constatez que vous ne faites pas confiance à ce CA. Il faut maintenant installer ce certificat. Les étapes suivantes sont nécessaires :



Il faut ensuite installer le certificat client :





Les certificats installés sous windows peuvent être accédés via la commande « mmc » (lancée comme une commande DOS) :



Fermer

Il faut ensuite choisir le sous-menu « Ajouter / Supprimer un composant logiciel enfichable »:



e lent Terminer Annuler

On peut alors accéder aux certificats personnels, ainsi qu'aux autorités de certification de confiance installée sur votre station.



On peut utiliser cet utilitaire pour supprimer les certificats.

4.6. Installation des certificats côté serveur, et lancement du serveur radius

L'ensemble des fichiers de configuration du serveur Radius se trouve dans le répertoire /etc/freeradius. Les deux certificats serveur et racine (serveur.pem et root.pem) doivent être installés dans le répertoire /etc/freeradius/certs. Il faut ensuite modifier trois fichiers du répertoire /etc/freeradius :

- **eap.conf** : configuration d'EAP
- clients.conf : configuration des APs ou commutateurs relayant EAP et autorisé à contacter le serveur Radius
- users : configuration des utilisateurs à authentifier

Dans le fichier **eap.conf**, on spécifie l'emplacement des certificats, et le type de version d'EAP utilisée.

```
default_eap_type = tls
tls {
    private_key_password = secretserver
    private_key_file = ${raddbdir}/certs/server.pem
    certificate_file = ${raddbdir}/certs/server.pem
    CA_file = ${raddbdir}/certs/root.pem
    dh_file = ${raddbdir}/certs/dh
    random_file = ${raddbdir}/certs/random
    fragment_size = 1024
    include_length = yes
    check_crl = no
}
```

Dans le fichier **clients.conf**, on définit l'AP et le commutateur comme équipement autorisé à relayé des messages EAP vers le serveur Radius. Par exemple :

```
client 192.168.150.0/24 {
    secret = tp
    shortname = ap-wifi
    nastype = other
}
```

Important : le paramètre « secret » (=tp dans l'exemple) est un mot de passe partagé avec l'AP, qui va être utilisé pour chiffrer les messages Radius échangé entre l'AP et le serveur. Il doit donc être configuré avec une valeur identique, au niveau de l'AP WiFi.

Dans le fichier **users**, on spécifie la liste des utilisateurs autorisés à se connecter. Ainsi, pour le certificat « client » généré précédemment, on ajoute la ligne suivante :

« client » Auth-Type := EAP, EAP-Type := EAP-TLS

Après cela, vous pouvez lancer le serveur Radius :

freeradius -X, le paramètre -X est optionnel et lance les messages de *debug*.

Votre serveur Radius attend maintenant vos demandes de connexion.

4.7. Configuration de l'AP

Au travers de l'interface WEB de l'AP, définissez les caractéristiques du serveur radius (au niveau de l'onglet « server manager ») :

	SERVER MANAGER	GLOBAL PROPERTIES		
HOME EXPRESS SET-UP	Hostname ap			ap uptime is 17 minutes
EXPRESS SECURITY NETWORK MAP	Security: Server Manager			
ASSOCIATION	Backup RADIUS Server			
INTERFACES SECURITY	Backup RADIUS Server:	(Hostname or IP Address)		
Admin Access	Shared Secret:			
SSID Manager				Apply Delete Cancel
Server Manager Local RADIUS Server	Corporate Servers			
Advanced Security SERVICES	Current Server List			
WIRELESS SERVICES	RADIUS ÷			
EVENTLOG	< NEW >	Server:	192.168.100.3 (Hostname or IP Address)	
		Shared Secret:	••	
	Delete	Authentication Port (optional):	1812 (0-65536)	
		Accounting Port (optional):	1813 (0-65536)	
				Apply Cancel

Mettre tp comme mot de passe partagé avec le serveur Radius.

Puis validez l'utilisation de ce serveur Radius pour l'authentification 802.1x/EAP :

Default Server Priorities	
EAP Authentication	MAC Authentication
Priority 1: 192.168.100.3 +	Priority 1: <pre>< NONE ></pre>
Priority 2: < NONE > \$	Priority 2: <pre>< NONE ></pre>
Priority 3: < NONE > +	Priority 3: <pre>< NONE > \$</pre>
Admin Authentication (RADIUS)	Admin Authentication (TACACS+)
Priority 1: < NONE > \$	Priority 1: <pre>< < NONE > \$</pre>
Priority 2: < NONE > \$	Priority 2: <pre>< NONE > \$</pre>
Priority 3: <pre>< NONE > \$</pre>	Priority 3: <pre> < NONE > \$</pre>

Et enfin, au niveau de la configuration du SSID V200-X attaché au VLAN 200, activez l'authentification « open + EAP », et supprimer la clé TKIP, fournie dynamiquement par le serveur Radius :

SID Properties			
Current OOID List			
< NEW >	SSID:	V100-1	
/200-1	VLAN:	100	
	Interface:	Radio0-802.11G	
	Network ID:	(0-4096)	
Delete			
lient Authentication Settings			
Methods Accepted:			
Open Authentication:	with EAP +		
Shared Authentication:	< NO ADDITION> ÷		
Network EAP:	< NO ADDITION >		
Server Priorities:			
Ear Authentication Servers	MAC Authentication	Servers	
Use Defaults Define Defaults	• Use Defaults	fine Defaults	
Cristomize	O Customize		
Priority 1: <pre> < NONE ></pre>	Priority 1:	IONE > \$	
Priority 2: < NONE > \$	Priority 2:	IONE >	
Priority 3: <pre> < NONE ></pre>	Priority 3: < M	IONE > \$	
lient Authenticated Key Management			
Key Management:	Mandatory ÷	ССКМ	S WPA

4.8. Configuration du SSID

Cliquez sur le SSID V200-X dans les réseaux favoris de votre carte WiFi, afin d'en modifier les propriétés :

En plus de basculer le SSID en WPA *enterprise*, vous devez paramétrer l'onglet **authentification**, sélectionnez le type EAP retenu, et cliquer sur le bouton **Propriétés** :

v20 Propriétés 🛛 ? 🔀		
Association Authentification Connexion		
Sélectionnez cette option pour fournir un accès réseau authentifié pour les réseaux Ethernet sans fil.		
Activer l'authentification IEEE 802.1X pour ce réseau		
Type EAP :		
Propriétés		
 Authentifier en tant qu'ordinateur lorsque les informations de l'ordinateur sont disponibles 		
Authentifier en tant qu'invité lorsque les informations concernant l'ordinateur ou l'utilisateur ne sont pas disponibles		
OK Annuler		

Sélectionnez le CA « de confiance » que nous avons généré, et choisissez l'option « Utiliser un nom d'utilisateur différent pour la connexion » (qui permet de bloquer la connexion EAP-TLS et de choisir le nom du certificat « client » envoyé au serveur Radius au moment du rattachement à l'AP). Sortir ensuite des propriétés de la carte WiFi).

Pr	opriétés des cartes à puce ou des autres certifi ? 🗙
	Lors de la connexion :
	🔿 Utiliser ma carte à puce
	 Utiliser un certificat sur cet ordinateur
	Utiliser la sélection de certificat simple (recommandé)
	Valider le certificat du serveur
	Connexion à ces serveurs :
	Autorités de certification racines de confiance :
	Class 3 Public Primary Certification Authority
	Class 3P Rimary CA
(Class 3TS Prinary CA
	Cours-WiFi
	Deutsche Telekom Root LA 1
	Deutsche Telekom Root LA 2
	DST (NRF) RootLA
	Afficher le certificat
Ľ	
	OK Annuler

Attendre maintenant la reconnexion vers le SSID et cliquer sur la bulle :



Choisir le certificat et observer les *logs* au niveau du serveur radius :

Connecter Connexion réseau sans fil 🛛 🔹 💽				
Nom de l'utilisateur sur le certificat :				
client1 💌				
Nom convivial :				
Émetteur :	Cours-WiFi			
Date d'expiration :	02/05/2009 22:35:36			
Nom d'utilisateur pour la connexion :				
client1				
	OK Annuler Afficher le certificat			