SUJET : **Mise en place d'un réseau Wifi avec authentification basée sur des certificats**

Réalisé par : - Daghsen Belgacem

-Hdider Makram

PROJET DE FIN D'ETUDES

(Licence Appliquée en Sciences et technique de l'information

et de communication)

Université Virtuelle de Tunis

A.U 2010-2011

DEDICACES

En termes de reconnaissance pour leurs sacrifices et en témoignage de mes profonds sentiments à leur égard, je dédie ce travail à :

Mes parents ;

Tous mes frères, sœurs, cousins et cousines ;

La famille DAGHSEN ;

Tous mes enseignants de l'UVT qui trouvent ici l'expression de mon profond respect ;

Mes amis ;

Mes camarades de promotion ;

Mes chers collègues du bureau d'emploi et du travail indépendant d'elhamma ;

Enfin, tous ceux que je n'ai pas pu citer.

DAGHSEN Belgacem

DEDICACES

En termes de reconnaissance pour leurs sacrifices et en témoignage de mes profonds sentiments à leur égard, je dédie ce travail à :

Mes parents et ma femme;

Tous mes frères, sœurs, cousins et cousines ;

La famille Hdider , La famille Hassine;

Tous mes enseignants de l'UVT qui trouvent ici l'expression de mon profond respect ;

Mes amis ;

Mes camarades de promotion ;

Mes chers collègues au rectorat de Gabès

Enfin, tous ceux que je n'ai pas pu citer.

HDIDER Makram

REMERCIEMENTS

Nous avons le plaisir de présenter nos sincères remerciements à notre encadreur : Mr Agoubi Belgacem Secrétaire général à l'institut supérieur des sciences et technique de l'eau de Gabès pour son aide et son précieux conseil durant toute la période de réalisation de ce projet.

Nous voudrons également exprimer notre gratitude à tous ceux qui ont contribué à la mise en œuvre de ce travail pour leurs disponibilités ainsi que l'institut supérieur des sciences et techniques de l'eau de Gabès où nous avons réalisé notre projet de fin d'étude.

Nous tenons enfin, à remercier vivement tous les membres du jury pour l'honneur qu'ils ont fait en acceptant de juger ce modeste travail, ainsi que le personnel de l'UVT qui ont veillé à notre formation.

SOMMAIRE

PRESENTATION DE L'INSTITUT (ISSTEG) 1
INTRODUCTION GENERALE 3
PARTIE I- ETUDE THEORIQUE 4
INTRODUCTION 5
CAHIER DES CHARGES 6
I- APERÇU DU RESEAU EXISTANT 7
II-CHOIX DE LA SOLUTION A DEPLOYER 10
1-Choix de l'architecture et de la norme du réseau 10
a- Le mode de fonctionnement 10
b- La norme de WIFI 11
c- Le nombre de points d'accès 13
d- Emplacement du point d'accès 13
2-Choix des paramètres de Sécurité 14
a-Modifier et Cacher le nom par défaut du réseau 14
b-Choisir un mot de passe d'accès au point d'accès 15
c-Filtrer les équipements par adressage MAC 15
d-Choisir une clé de chiffrement hautement sécurisée 15
e-Choisir une méthode d'authentification basée sur des certificats 16
III-COMPOSANTS MATERIELS ET LOGICIELS 18
1- Identification des composants matériels 18
a- Les adaptateurs de réseau clients sans fil 18
b- Les points d'accès sans fil WIFI 19
c- Le serveur 20
2- Identification des composants logiciels 21

IV- PRESENTATION DE LA SOLUTION RETENUE 22
1- Conception physique 22
2- Conception logique 23
PARTIE II- ETUDE PRATIQUE 25
I- MISE EN PLACE DE LA SOLUTION RETENUE 26
1- Plan d'adressage 26
2- Installation d'une autorité de certificat racine 26
a- Installation des Service IIS 26
3- Installation et configuration du serveur RADIUS 30
a- Création d'un utilisateur et d'un groupe dans active Directory 31
b- Configuration du serveur RADIUS 33
4- Installation et sécurisation du point d'accès WIFI 37
5- Configuration d'un client d'accès WIFI 39
a- Installation du certificat auto signé d'authentification et du certificat d'un utilisateur 39
b- Configuration de la connexion réseau sans fil 42
II- OBSERVATIONS ET TESTS 44
CONCLUSION 46
BIBLIOGRAPHIE 47
ANNEXES 48

PRESENTATION DE L'INSTITUT (ISSTEG)

1- Création

ISSTEG (Institut supérieur des sciences et techniques de l'eau de Gabès), créé en 2005, par le décret N° 1971 du 14 juillet 2005, l'Institut Supérieur des Sciences et Techniques de l'eau de Gabès est un établissement d'enseignement supérieur révélant de l'Université de Gabès.

L'ISSTEG a pour mission, la formation des étudiants dans le domaine des Sciences et Techniques des eaux. Il assure la formation en :

- Licence appliquée en Sciences et techniques de l'Eau, avec 3 parcours:

    1- Valorisation des ressources en eaux

    2- Techniques de forage et de pompage

    3- Géologie des systèmes aquifères

- Master professionnel LMD avec 2 parcours :

1. Gestion Intégrée des Ressources en Eau

2. Forage, Pompage et Réseaux Hydrauliques

- Master professionnel (Bac + 4) en Techniques de forage

2- Organigramme

- **Le directeur :** Mr Jedoui Younes

Le directeur de l'ISSTEG est celui qui veille d'une part sur la direction administrative et financière et d'autre part sur le côté scientifique et pédagogique de l'établissement.

- **Le secrétaire General :** Mr Agoubi Belgacem

Le secrétaire General de l'ISSTEG est le dynamo de l'établissement, il mène plusieurs rôles tels que :

- La direction des services administratifs et financiers de l'établissement,
- Le suivi du déroulement des études et des affaires estudiantines,
- La gestion du cadre enseignant, administratif, technique et ouvrier de l'ISSTEG

INTRODUCTION GENERALE

Dans le cadre du programme de formation « Licence appliquée en sciences et techniques de l'information et de communications » proposé par l'université virtuelle de Tunis (UVT), Les étudiants sont menés à effectuer en fin de l'année, un stage pratique dans une entreprise en vue de mettre en application les connaissances acquises tout au long de la période de formation afin de permettre une intégration facile et rapide de ses diplômés en milieu professionnel et de leur donner la chance de continuer ses études en mastères.. C'est ainsi que l'institut supérieur des sciences et techniques des eaux s'est portée garante pour nous accueillir et ainsi nous permettre au mieux de parfaire notre formation. Le présent rapport a pour but de présenter les différentes étapes que nous avons traversées tout au long de cette période et de détailler dans les moindres détails les différents travaux effectués lors de celle-ci. Comme l'indique le cahier de charge, il comportera deux grandes parties à savoir la partie d'étude théorique et la partie d'étude pratique.

PARTIE I : ETUDE THEORIQUE

INTRODUCTION

Sous les instructions de notre encadreur, nous avons été amenés à travailler sur le thème suivant : « Déploiement d'un réseau sans fil Wi-Fi avec authentification basée sur des certificats ».

Les réseaux informatiques sont devenus depuis quelques années, des axes majeurs de communication. Aujourd'hui, les principaux développements de ces réseaux visent à favoriser la mobilité, pour répondre aux nouveaux besoins des personnes, des téléphones et ordinateurs portables, qui sont par essence mobiles et qu'on retrouve de plus en plus dans la société.

Les réseaux sans-fil permettent à leurs utilisateurs de se connecter de n'importe où et d'accéder aux ressources de leurs réseaux pour tout ce qui sont à la portée de ceux-ci. Cependant, lorsqu'un réseau filaire existe déjà, une analyse des solutions existantes doit être menée afin que la sécurité, la performance et la qualité du réseau global soient de rigueur.

CAHIER DES CHARGES

Ce projet de fin d'études est :

Proposé et encadré par : Mr Agoubi Belgacem

Réalisé par : - **Daghsen Belgacem**

- **Hdider Makram**

TITRE DU PROJET :

Mise en place d'un réseau Wifi avec authentification basée sur des certificats

DESCRIPTION DU PROJET :

- Caractéristiques principales du réseau à implémenter,
- Etude de différentes solutions techniques et choix de la solution,
- Réflexion sur l'architecture et le fonctionnement du réseau
- Installation effective du réseau
- Mise en route du réseau

TRAVAIL DEMANDE :

- Etude bibliographique
- Conception
- Réalisation
- Rapport

I. APERÇU DU RESEAU EXISTANT

L'ISSTEG est un bâtiment qui comprend trois étages avec un sous-sol, Seul deux salles (1er étage) sont câblées en filaire (LAB1 et LAB C2I) à partir de 2 baies de brassage (Switch2, Switch3) interconnectés via une liaison câblée au répartiteur général (RDC). Les bureaux administratifs, enseignants sont liés au réseau à travers des connexions wifi.

La Bibliothèque situé au sous-sol n'est pas encore reliée au réseau de l'établissement ce qui empêche une majorité d'étudiants, de se connecter à internet.

Pour les salles et les bureaux actuellement connectées au réseau local, aucune politique de contrôle d'accès n'a été mise en place. Le partage des données et des ressources matérielles s'effectuent via le groupe de travail « **ISSTEG**». Un serveur Windows 2003 Server est installé et qui joue le rôle de passerelle (Serveur DHCP). L'adressage des postes est automatique.

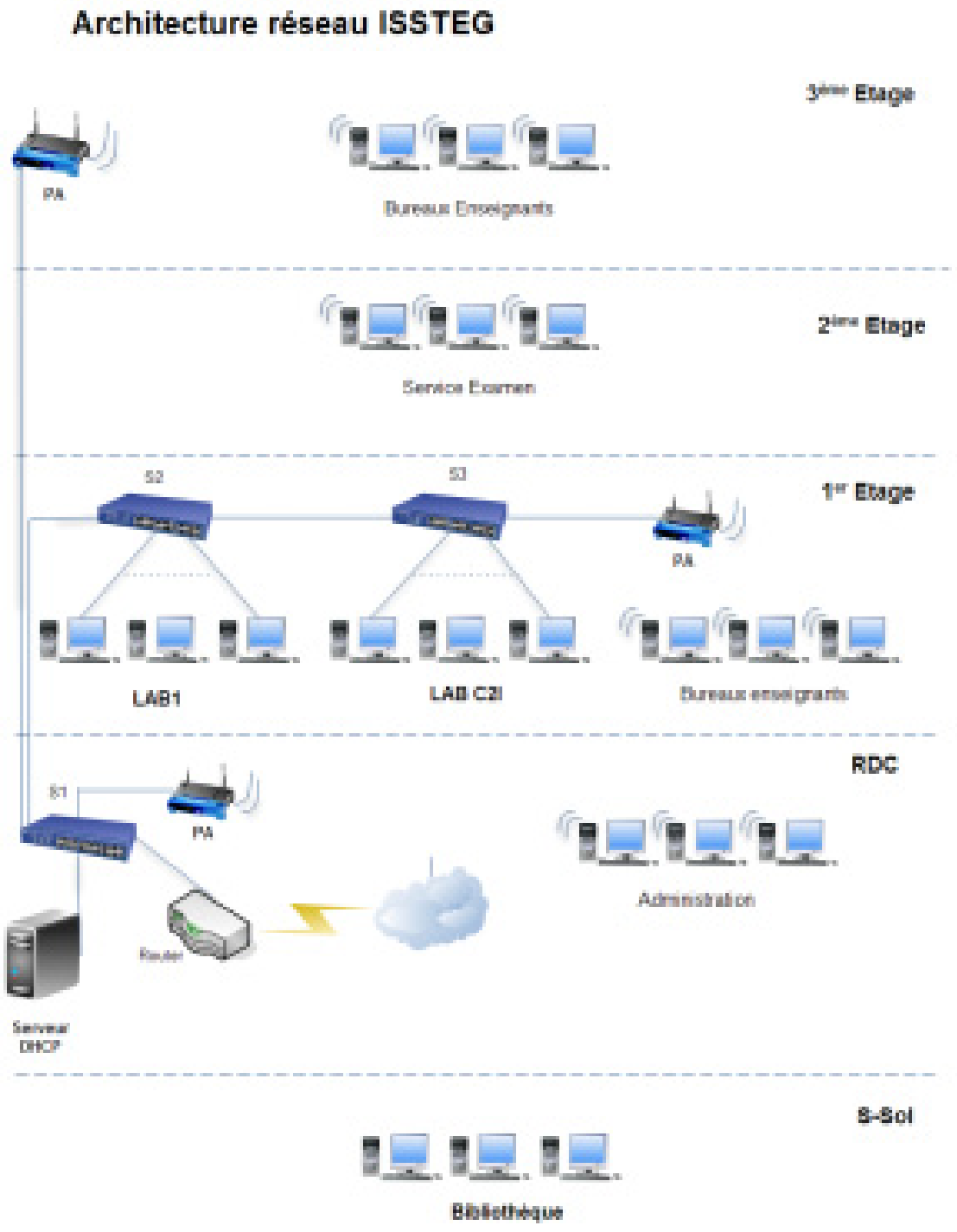


Schéma du réseau existant

A la question de savoir les raisons ayant favorisé le choix de ce projet, il nous a été répondu par plusieurs points. Notamment, le bâtiment actuellement exploité par l'ISSTEG est alloué c'est à dire il n'est pas une construction publique et non destiné dès le début de sa construction à l'enseignement ce qui justifie l'absence du câblage informatique dans la plupart des salles de l'institut sauf dans quelques bureaux qui sont câblés sous le budget de l'établissement. Et afin d'éviter un câblage couteux et fastidieux nécessitant des percées de trous dans les murs, toutes les machines non interconnectées devront être configurées pour pouvoir accéder au réseau de l'établissement par le Wi-Fi.

Bien plus, il nous a été signalé la forte demande des étudiants de connexion à internet afin d'effectuer des recherches et de communiquer avec ses enseignants à travers ses ordinateurs portables.

Enfin, le problème de stabilité du local qui est actuellement exploité d'une façon provisoire en attendant la construction du propre bâtiment de l'ISSTEG qui est en phase d'étude ainsi il n'est pas exclut que l'on vienne à changer les locaux d'un moment à l'autre. Un réseau sans fil évitera les câblages répétitifs à chaque déménagement.

II. CHOIX DE LA SOLUTION A DEPLOYER

Le déploiement d'un réseau sans fil Wi-Fi doit passer par une étude détaillée des solutions existantes pour être en accord avec les principes évoquées dans le cahier de charge.

1- Choix de l'architecture et de la norme du réseau

Sur ces points, nous avons retenu les mesures suivantes:

a- Le mode de fonctionnement

Le Wi-Fi peut fonctionner suivant 2 modes : ad hoc et infrastructure. En mode ad hoc, il n'y a pas d'infrastructure quelconque à mettre en place. Les échanges entre clients Wi-Fi s'effectuent lorsqu'ils sont à portée d'ondes radios. Donc, il n'y a pas de sécurité possible dans un tel mode de fonctionnement. Cependant, en mode infrastructure, on se base sur une station spéciale appelée Point d'Accès (PA). Elle permet à une station Wi-Fi de se connecter à une autre station Wi-Fi via leur PA commun. Une station Wi-Fi associée à un autre PA peut aussi s'interconnecter. L'ensemble des stations à portée radio du PA forme un BSS (Basic Service Set). Chaque BBS est identifié par un BSSID (BSS Identifier) de 6 octets qui correspond souvent à l'adresse MAC du PA. Tout ceci permet de contrôler les connections au réseau afin d'y appliquer des politiques sécuritaires. Ainsi notre choix s'est porté sur le mode infrastructure.

b- La norme de Wi-Fi

Les normes de Wi-Fi sont nombreuses et diverses. De toutes ces normes, les plus connues sont 802.11a, 802.11b et 802.11g, qui sont les principales du standard 802.11 ceci grâce à leur large intégration dans les matériels et logiciels.

- **802.11a**

La norme 802.11a permet d'obtenir un débit théorique de 54 Mbps, soit cinq fois plus que le 802.11b, pour une portée d'environ une dizaine de mètres seulement. La norme 802.11a s'appuie sur un codage du type OFDM sur la bande de fréquence 5 GHz et utilise 8 canaux. Les équipements 802.11a ne sont pas compatibles avec les équipements 802.11b/g. Il existe toutefois des matériels intégrant des puces 802.11a et 802.11b, on parle alors de matériels «dual band».

Débit théorique (en intérieur)	Portée
54 Mbits/s	10 m
24 Mbits/s	30 m
12 Mbits/s	50 m

Portées et débits pour la norme 802.11a

- **802.11b**

La norme 802.11b permet d'obtenir un débit théorique de 11 Mbps, pour une portée d'environ une cinquantaine de mètres en intérieur et jusqu'à 200 mètres en extérieur (et même au-delà avec des antennes directionnelles).

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
11 Mbits/s	50 m	200 m
5,5 Mbits/s	75 m	300 m
2 Mbits/s	100 m	400 m
1 Mbit/s	150 m	500 m

Portées et débits pour la norme 802.11b

- **802.11g**

La norme 802.11g permet d'obtenir un débit théorique de 54 Mbps pour des portées équivalentes à celles de la norme 802.11b. D'autre part, dans la mesure où la norme 802.11g utilise la bande de fréquence 2,4GHZ avec un codage OFDM, cette norme est compatible avec les matériels 802.11b, à l'exception de certains anciens matériels.

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
54 Mbits/s	27 m	75 m
24 Mbit/s	42 m	140 m
12 Mbit/s	64 m	250 m
6 Mbit/s	90 m	400 m

Portées et débits pour la norme 802.11g

Remarque : Avec les normes 802.11b+ et 802.11g+, on atteint respectivement des débits théoriques de 22 Mbit/s et 108 Mbits/s.

En somme, nous disposons des équipements intégrants les normes 802.11b/g c'est qui nous donne des débits et des portées acceptables dans notre cas.

c- Le nombre de point d'accès

Actuellement on retrouve à l'ISSTEG 3 points d'accès situés respectivement au RDC, 1er étage et 3ème étage et qui couvrent les bureaux et les salles concernés. La bibliothèque situé au sous-sol est l'espace qui concerne les étudiants et qui nécessite l'ajout d'un quatrième point d'accès puisqu' il n'est pas couvert par les ondes WIFI qui viennent du RDC. Notre étude se fera donc pour un nombre d'étudiants compris entre 10 et 30. Avec 10 clients Wi-Fi et 1 points d'accès satisfaisant la norme 802.11g on obtient en théorie un débit de l'ordre de 10Mbits/s pour chacun. Si ce nombre de clients doit évoluer par exemple jusqu'à 30, on aura alors sensiblement 3Mbits/s pour chacun ce qui reste totalement acceptable.

d- Emplacement du point d'accès

Nous savons qu'avec la norme 802.11g+, pour un débit théorique de 108Mbit/s on peut atteindre une trentaine de mètres en intérieur, or cette distance délimite parfaitement la zone à couvrir par le réseau qui ne dépasse pas les 20 mètres. Nous avons choisi d'installer le point d'accès au guichet de la bibliothèque qui est l'endroit qui est près du répartiteur général et où il est mieux protégé (loin de la portée des étudiants).

2- Choix des paramètres de sécurité

La sécurité des réseaux sans fil est l'élément essentiel qui décourage plusieurs personnes de déployer cette technologie. En effet, les ondes radios ne pouvant pas être réservées dans un espace délimitée, n'importe quelle personne se trouvant à portée de ces ondes peut s'y connecter et utiliser le réseau à des fins malfaisantes. Ainsi, il est essentiel de déployer de gros moyens pour sécuriser notre réseau sans fil Wi-Fi. Pour cela on a ainsi retenu les points suivants:

a- Modifier et Cacher le nom par défaut du réseau :

Un réseau Wi-Fi porte toujours un nom d'identification afin que les ordinateurs puissent le détecter et se connecter dessus. Ce nom s'appelle le SSID (Service Set IDentifier). Si on ne configure pas le point d'accès, le SSID est défini par défaut. Ainsi on le modifiera, afin de le reconnaître plus facilement par la suite.

Le SSID est une information importante pour se connecter au réseau sans fil. Le point d'accès diffuse continuellement cette information pour permettre aux ordinateurs de le détecter. Le SSID n'est pas une fonction de sécurisation mais permet de rendre "caché" son point d'accès à la vue de tout le monde. Une fois le réseau configuré avec les ordinateurs, on activera la fonction "cacher le SSID", présente dans le point d'accès, afin de rendre ce dernier "invisible" au monde extérieur.

b- Choisir un mot de passe d'accès au point d'accès

L'administration du point d'accès se fait par l'intermédiaire d'une interface Web accessible par n'importe quel ordinateur connecté par câble ou par Wifi. Il suffit de saisir une adresse IP (fournie par le constructeur) dans le navigateur Web et le mot de passe par défaut (fourni par le constructeur) pour accéder à l'administration. A ce stade, toute personne pouvant accéder au réseau, peut faire les changements ou modifier d'autres paramètres du point d'accès. On changera donc le mot de passe par un nouveau. Ce mot de passe devra répondre au principe de mots de passe forts.

c- Filtrer les équipements par adressage MAC

Une adresse MAC (Media Access Control) permet d'identifier matériellement un ordinateur grâce à son adaptateur réseau. Cette adresse est unique et définie par le fabriquant de l'adaptateur. Chaque point d'accès offre la possibilité d'utiliser le filtrage MAC. L'adaptateur qui n'a pas son adresse MAC dans la liste autorisée ne sera pas autorisé à se connecter sur le réseau. Notons tout de même que le filtrage d'adresses MAC est contournable. En effet, une adresse Mac peut être émulée sous un environnement Linux ou même Windows.

d- Choisir une clé de chiffrement hautement sécurisée

Deux types de cryptage de donnée existent actuellement : WEP (Wired Equivalent Privacy) et WPA (Wi-Fi Protected Access**).**

- Le cryptage WEP : est un protocole de sécurité pour les réseaux sans fil. WEP offre un niveau de sécurité de base mais satisfaisant pour la transmission de données sans fil.
- Le cryptage (WPA et WPA2) : est un mécanisme pour sécuriser les réseaux sans-fil de type Wi-Fi. Il a été créé en réponse aux nombreuses et sévères faiblesses que des chercheurs ont trouvées dans le mécanisme précédent, le WEP, le WPA sécurise la transmission de données sans fil en utilisant une clé similaire à la clé WEP, mais sa force est que cette clé change dynamiquement. Il est donc plus difficile pour un pirate de la découvrir et d'accéder au réseau.

On choisira donc WPA pour le chiffrement puisqu' il est compatible avec nos équipements existants. On aurait pu utiliser le WPA2 mais bien que son implémentation puisse engendrer des problèmes de compatibilité, on l'a évité.

e- Choisir une méthode d'authentification basée sur des certificats

L'EAP (Extensible Authentification Protocol) n'est pas un protocole d'authentification à proprement parler, mais un protocole de transport de protocoles d'authentification tels que TLS, MD5, PEAP, LEAP, etc. En effet, avec cette méthode, les paquets du protocole d'authentification sont encapsulés dans les paquets EAP.

Son but est l'authentification d'un utilisateur sur un réseau non ouvert, car dans un premier temps, dans ce type de réseau, seul les trafics EAP sont permis (pour permettre l'authentification). Ce n'est qu'après authentification que le réseau est ouvert. Une méthode

d'authentification EAP utilise différents éléments pour identifier un client tels que : le couple « login/mot de passe », les « certificats électroniques », les « cartes à puces (SIM) », etc....

En plus de l'authentification, EAP gère la distribution dynamique des clés de chiffrement (WEP ou WPA). Les deux méthodes d'authentification EAP utilisant des certificats sont :

PEAP (Protected EAP): Le processus d'authentification de PEAP consiste à établir un tunnel sécurisé TLS entre le client et le serveur d'authentification, en authentifiant le serveur RADIUS à l'aide d'un certificat. Ensuite, il est possible de choisir entre la méthode MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) ou TLS pour authentifier l'utilisateur. Quand la méthode PEAP est utilisée c'est souvent pour éviter d'utiliser les certificats client, il est donc logique que sur les deux méthodes proposées par PEAP, l'utilisation de Login/Password, via MS-CHAP, soit largement privilégiée.

EAP-TLS (EAP-Transport Layer Security): EAP-TLS est une méthode d'authentification mutuelle, ce qui signifie que le client et le serveur se prouvent respectivement leur identité. Lors de l'échange EAP-TLS, le client d'accès à distance envoie son certificat d'utilisateur et le serveur d'accès à distance envoie son certificat d'ordinateur. Si l'un quelconque des certificats n'est pas envoyé ou n'est pas valide, la connexion est interrompue. Rappelons que TLS, la version normalisée de SSL (Secure Socket Layer), est un protocole de transport sécurisé (chiffrement, authentification mutuelle, contrôle d'intégrité).

Nous utiliserons donc la méthode EAP-TLS qui propose le plus de sécurité. Avec la méthode EAP-TLS l'authentification du client d'accès peut se faire de différentes façons :

a- A l'aide d'un certificat personnel associé à la machine, l'authentification a lieu au démarrage de la machine.

b- A l'aide d'un certificat personnel associé à l'utilisateur, l'authentification a lieu après l'entrée en session de l'utilisateur.

Nous avons opté pour la seconde méthode car elle augmente le niveau de sécurité.

III- Composants matériels et logiciels

1- Identification des composants matériels :

a- Les adaptateurs de réseau client sans fil

Les cartes réseaux PCI installés ont les caractéristiques techniques suivantes :

- Compatible Linux, MAC OSxxx et Windows XP/2000/98 SE/ME, certifié pour Windows Vista ;
- Standard 802.11g et compatibilité rétrograde avec les produits en 802.11b ;
- Taux de transfert des données sans fil pouvant atteindre 54 Mbps;
- Cryptages WEP, WPA et WPA2 supportés ;
- Antenne externe

Carte réseau PCI

b- Les points d'accès sans fil Wi-Fi

Nous disposons des points d'accès de référence D-Link DWL-3200AP ayant les caractéristiques suivantes :

* Standard 802.11g 2,4GHz (108Mbps).

* Taux de transfert des données : connexion sans fil à 11 MBits/s (norme IEEE 802.11b), 54 Mbits/s (norme IEEE 802.11g) et 108 Mbits/s avec les appareils compatibles Super G de la gamme D-Link.

* Port Ethernet sur RJ-45 compatible Q802.3af PoE.

* Compatible avec les équipements 802.11b sans fil existants.

* Compatible réseau filaire.

* Power Over Ethernet (PoE) integré.

* Encryptage de données WEP 64/128/152 bits.

* Sécurité WPA avec authentification RADIUS 802.1x de l'utilisateur.

* Configuration et gestion à partir du web.

Point d'accès D-Link DWL-3200AP

c- Le serveur.

Le serveur utilisé a les caractéristiques suivantes :

Ressource	Configuration minimale
Processeur	Intel Dual core 1,6 Gigahertz (GHz)
Mémoire vive	1 Go (giga-octets)
Carte réseau	Deux cartes réseau
Disque dur	1 disque dur de 250 Go

Configuration matérielle minimale du serveur d'authentification

Serveur DELL 1800

2- Identification des composants logiciels :

Comme logiciels, on aura besoin :

- Un système d'exploitation serveur : Windows 2003 Server Entreprise Edition

Nous l'avons choisi car il inclut la gestion des certificats, il dispose d'un serveur RADIUS intégré sous le nom d'IAS (Internet Authentication Service) pouvant gérer un nombre infini de clients RADIUS; les couples login/mot de passe pourront être gérés avec l'annuaire Active Directory.

L'autre solution aurait été d'utiliser une distribution Linux, avec ce choix, on aurait utilisé FreeRadius pour l'authentification. Mais puisque les établissements universitaires ayants des conventions avec la société Microsoft et ayant des licences d'utilisation des ses produits, nous avons retenu la solution proposé par Windows 2003 Server et qui est installé dans le serveur de l'établissement mais sans profiter de plusieurs fonctions de ce système d'exploitation.

IV- Présentation de la solution retenue

1- Conception physique

En définitive, la solution retenue aura pour topologie physique le schéma suivant:

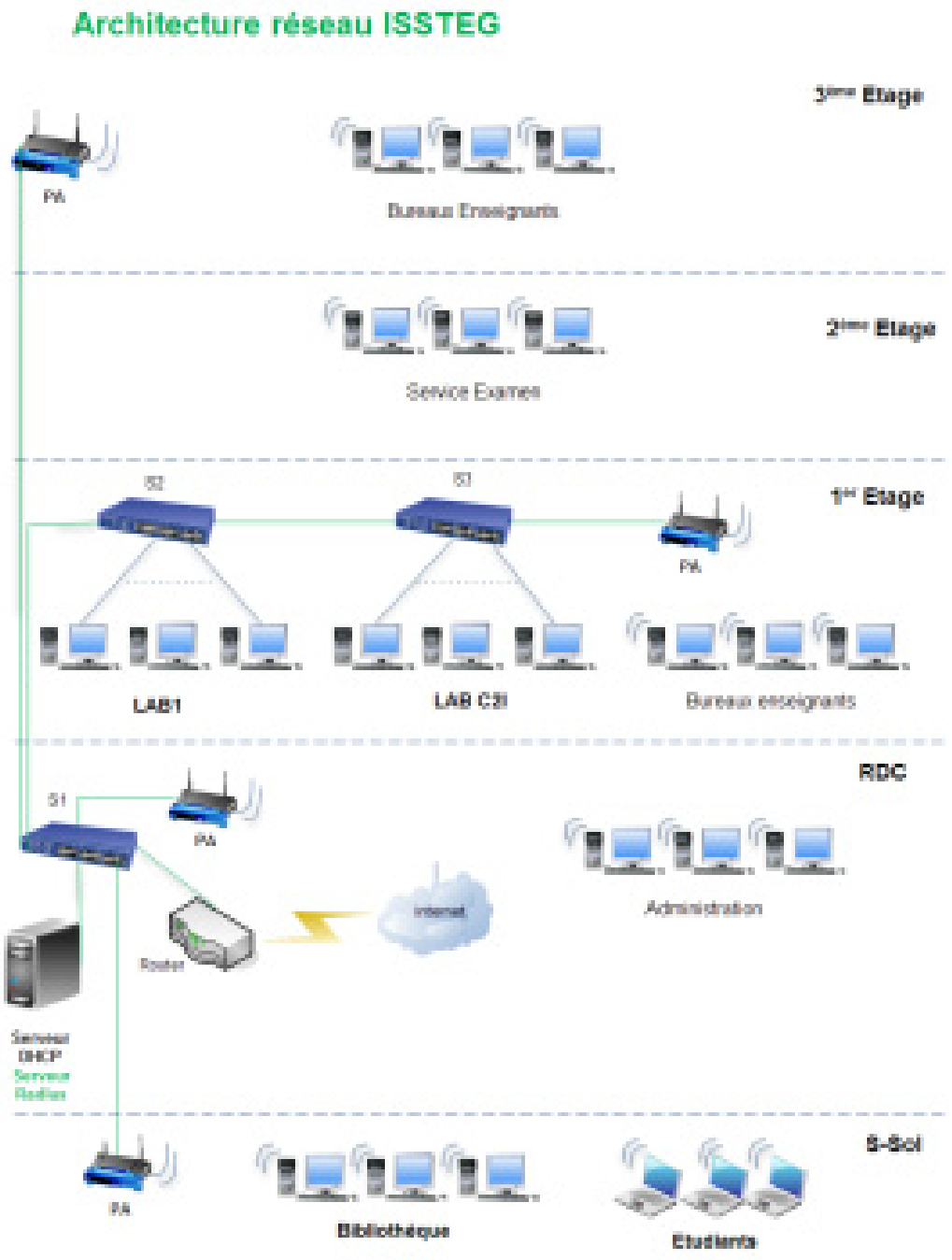


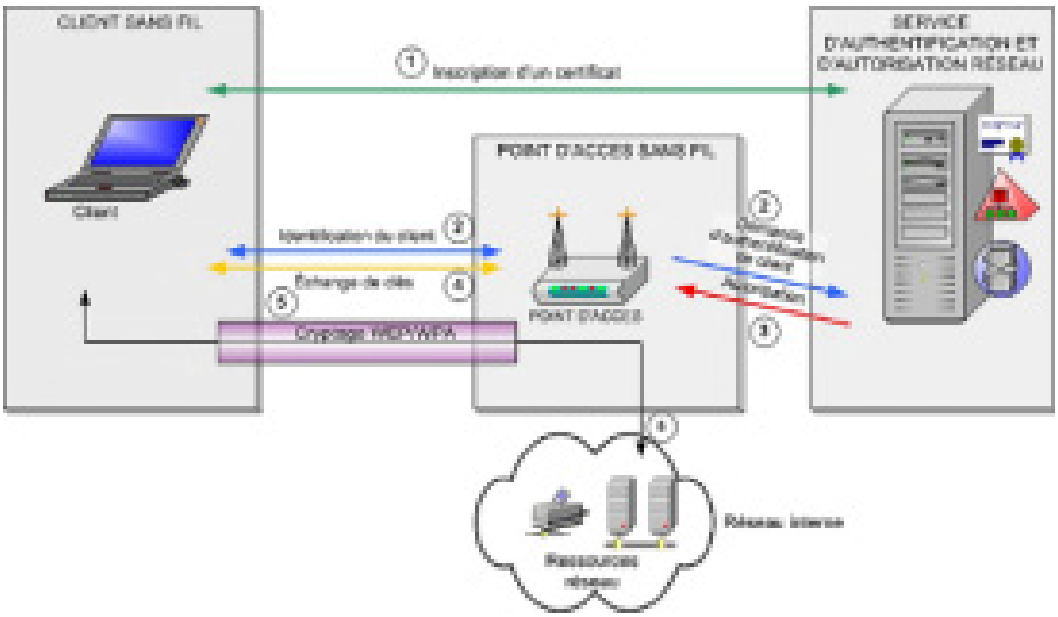
Schéma du réseau définitif

Description :

Comme on peut le remarquer, la mise en place du réseau sans fil et du serveur RADIUS ne va pas modifier l'architecture du réseau existant. Tous les ordinateurs de bureau et portables du réseau seront désormais connectés grâce au Wi-Fi. En effet, tous les ordinateurs portables récents incluent déjà l'adaptateur sans fil et ceux de l'ISSTEG n'échappent pas à la règle et sont équipés par des adaptateurs de réseau client sans fil compatible 802.1x.

2- Conception logique

Le diagramme ci-dessous illustre la conception de la solution choisie (authentification EAP-TLS 802.1X).



Concept de solution basé sur l'authentification

EAP-TLS 802.1X

Ce diagramme décrit quatre composants principaux :

Le client sans fil. Il s'agit d'un ordinateur ou d'un périphérique exécutant une application qui doit accéder à des ressources du réseau. Ce client est capable non seulement de crypter son trafic réseau, mais aussi de stocker et d'échanger des informations d'identité (clés ou mots de passe).

Le point d'accès sans fil. Dans la terminologie réseau, on parle également de service d'accès au réseau. Ce point d'accès sans fil gère l'accès au réseau et crypte le trafic sans fil. Il permet d'échanger en toute sécurité des clés de cryptage avec le client, afin de sécuriser le trafic du réseau. Enfin, il peut interroger un service d'authentification et d'autorisation pour autoriser ou refuser l'accès au réseau.

Le service NAAS (Network Authentication and Authorization Service). Ce service stocke et vérifie l'identité des utilisateurs habilités, et gère les accès conformément à la stratégie de contrôle d'accès définie. Il peut également collecter des informations de comptabilité et d'audit sur l'accès du client au réseau.

Le réseau interne. Il s'agit d'une zone sécurisée de services réseau, à laquelle l'application cliente sans fil doit avoir accès.

PARTIE II : ETUDE PRATIQUE

I. Mise en place de la solution retenue

1- Plan d'adressage

Notre réseau va conserver le même plan d'adressage de l'établissement afin d'éviter la perturbation ou la rupture de l'accès au réseau et aux ressources.

Adresse sous réseau : 192.168.1.0

Masque du sous réseau : 255.255.255.0

Adresse du serveur : 192.168.1.1

Adresse des points d'accès : 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.5

Adresses des postes clients : 192.168.1.70 - 192.168.1.255

2- Installation d'une autorité de certificat racine

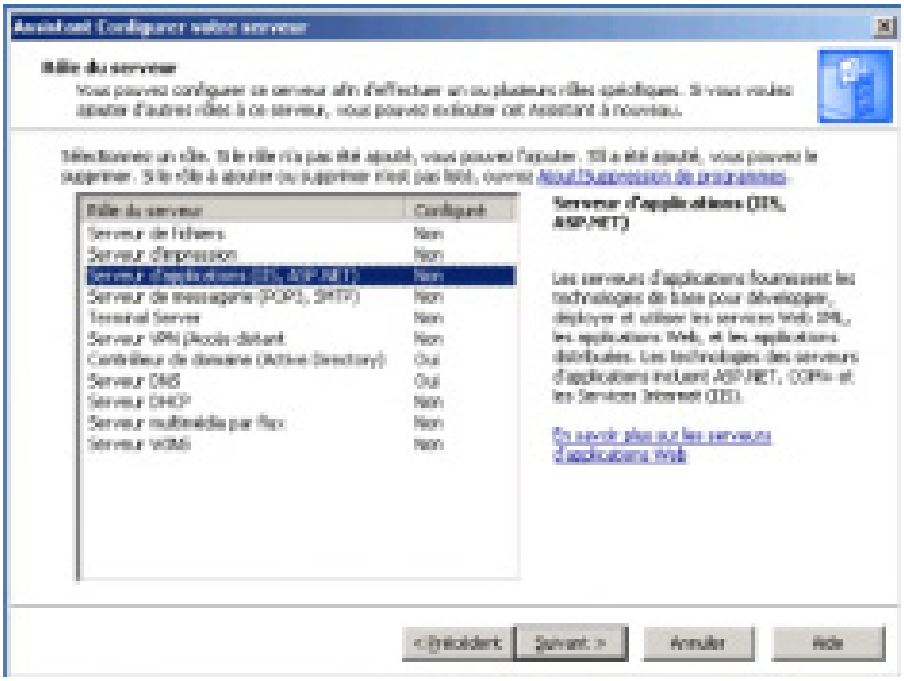
Au préalable le serveur de noms devra être installé. En effet il n'y a pas d'autorité de certification sans DNS (Domain Name System).

L'installation d'une autorité de certificat racine nécessite tout d'abord l'installation des services IIS (Internet Information Server).

a- Installation des Services IIS

L'installation des Services IIS peut s'effectuer de la manière suivante :

Par l'outil " Gérer votre serveur " situé dans les outils d'administration. Après ajouter un rôle à notre serveur, on choisit Serveurs d'application (IIS, ASP.NET).

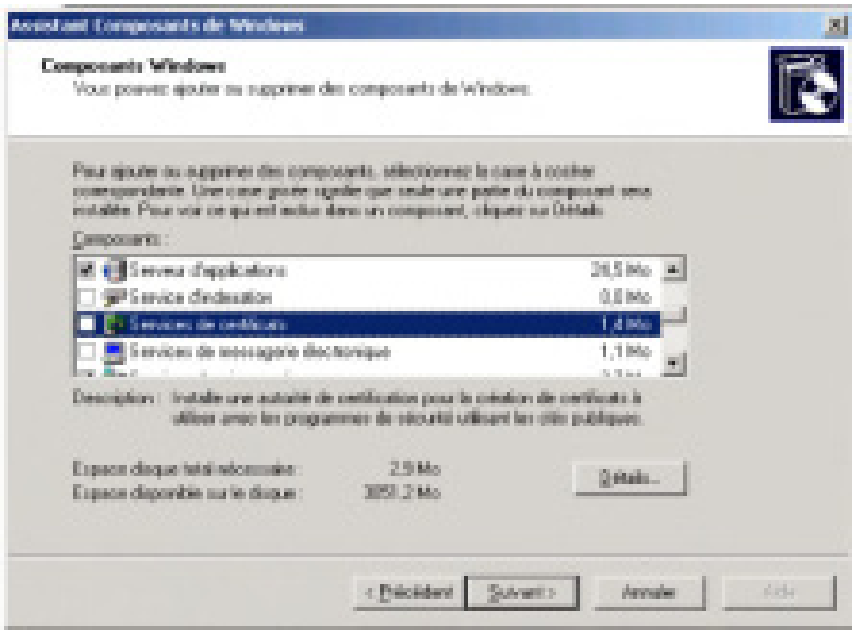


Puis nous avons le choix d'installer les extensions du serveur FrontPage et/ou la structure ASP.NET. Dans notre cas nous utiliserons ASP.NET car l'autorité de certificat nécessite cette technologie. L'installation va se poursuivre jusqu'à la fin.

Ensuite, nous allons pouvoir installer une Autorité de Certification Racine.

Nous utilisons l'outil " Ajout/Suppression de composants Windows " situé dans " Ajout/Suppression de programmes " du Panneau de configuration.

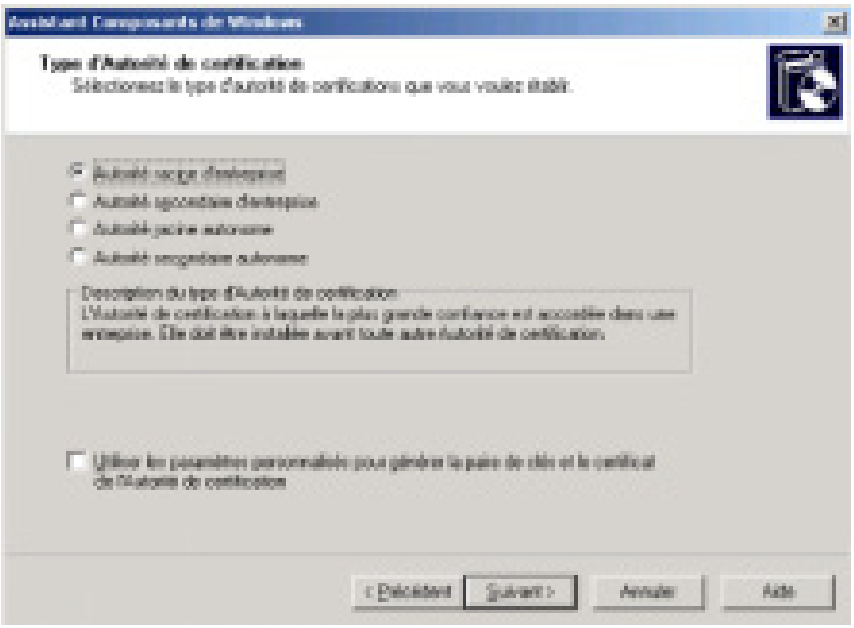
Puis on sélectionne Services de certificats



Un message d'erreur apparaît et stipule qu'après installation des Services de certificats l'ordinateur ne devra ni changer de nom ni changer de domaine car les certificats émis par notre autorité risqueraient de ne plus être valides.

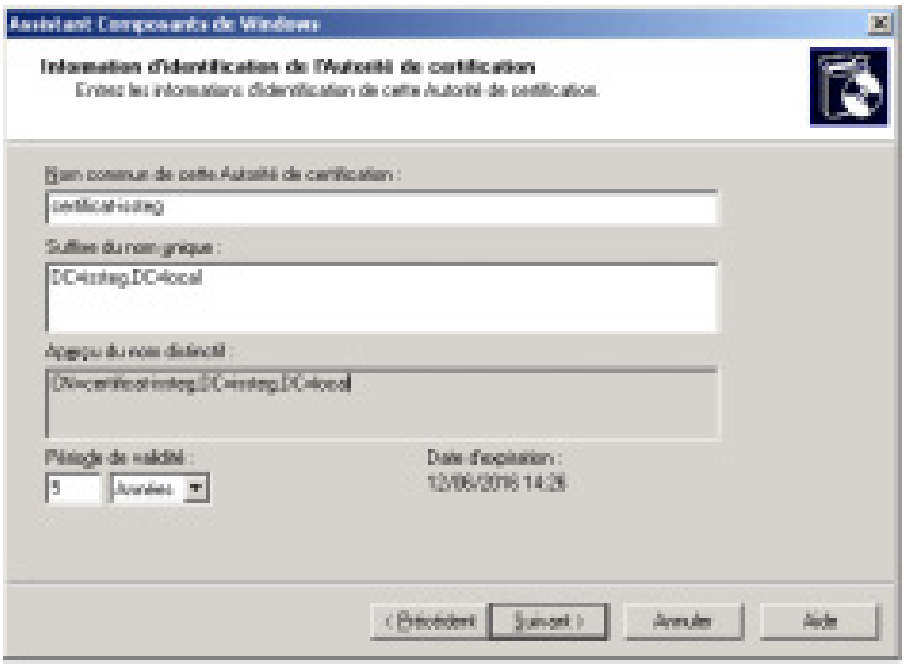
Nous validons par oui puis continuons l'installation.

Ensuite, on sélectionne le type d'autorité de certification. Nous choisissons **Autorité racine d'entreprise** car il s'agit de la première autorité installée.

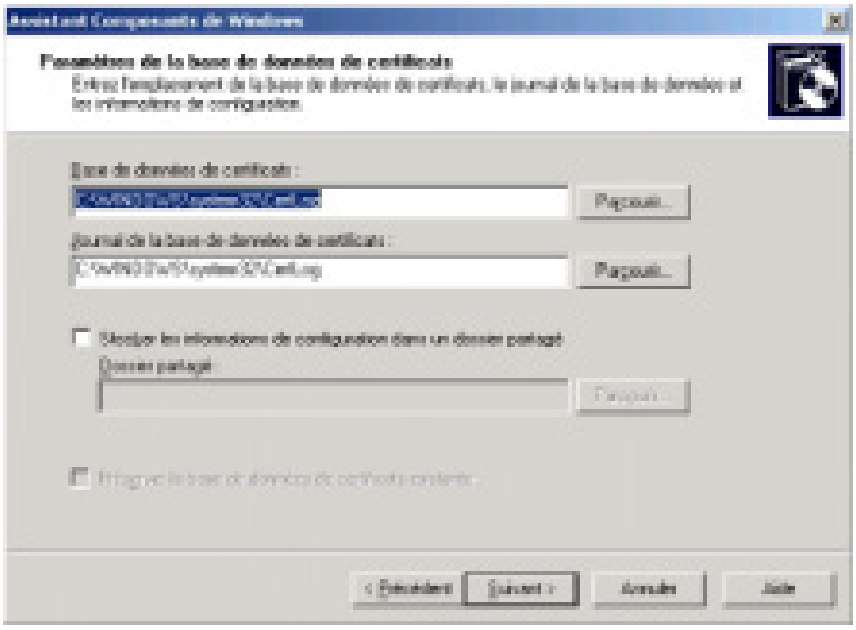


L'installation continue, il faut alors choisir le nom de notre autorité.

Dans notre cas nous choisissons : **certificat-issteg**.



Puis on sélectionne l'**emplacement de la base de données** et le **journal de certificats : C:\WINDOWS\system32\Certlog**



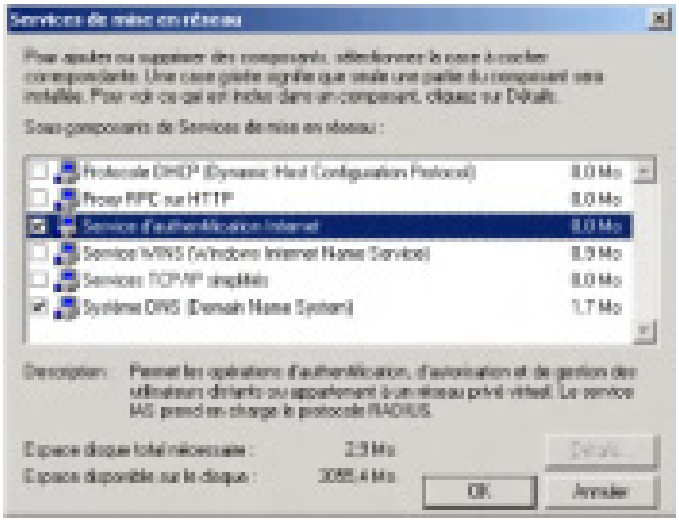
Une alerte signale que pour continuer l'installation, les Services IIS doivent être temporairement arretes. On valide donc par oui.

L'installation nous signale qu'ASP doit être activé pour permettre aux services de certificats de fournir un service d'inscription par le Web. On valide par oui et l'installation des Services de certificat se poursuit et s'achève sans problème.

3- Installation et configuration du serveur radius

Nous utilisons l'outil " Ajout/Suppression de composants Windows " situé dans " Ajout/Suppression de programmes " du Panneau de configuration.

Nous sélectionnons par la suite **Services de mise en réseau**, puis dans détails il faut cocher **Service d'Authentification Internet**.



Puis l'installation continue.

Après l'installation, nous allons créer des comptes utilisateurs et un groupe dans Active Directory pour les utilisateurs du réseau Wi-Fi, avant de passer à la configuration du serveur Radius.

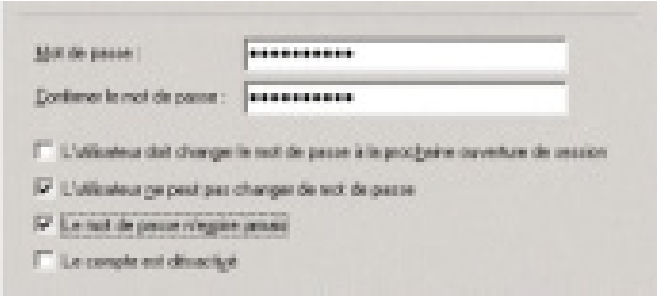
a- Création d'un utilisateur et d'un groupe dans Active Directory

Allez dans le menu Démarrer puis Outils d'administration et enfin sélectionner Utilisateurs et ordinateurs Active Directory.

Dans le dossier Users on fait un click droit avec la souris puis Nouvel utilisateur.

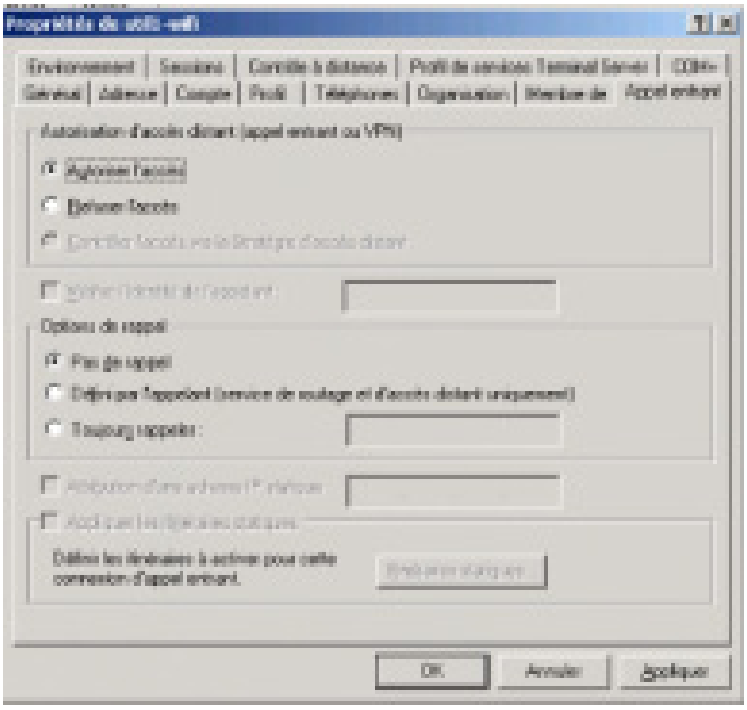
On crée alors un utilisateur **util1-wifi**.

On entre ensuite le mot de passe, ainsi que les options concernant le compte.



Puis on fait un click droit sur l'utilisateur util1-wifi, dans propriétés on va dans l'onglet **Appel entrant**.

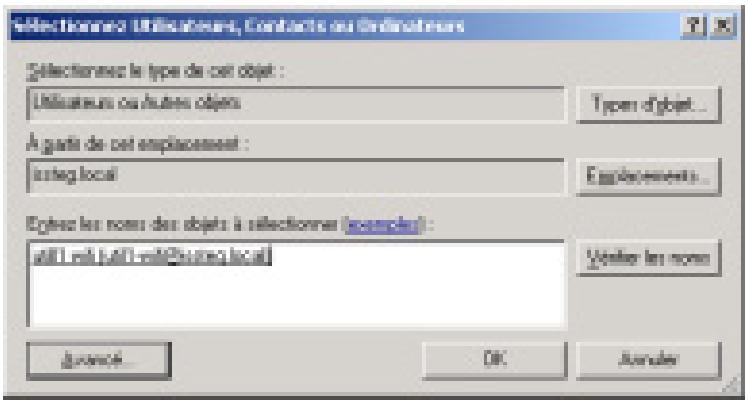
Puis dans **Autorisation d'accès distant** (appel entrant ou VPN) on coche **Autoriser l'accès**.



Nous pouvons maintenant créer un groupe d'utilisateurs qui contiendra les utilisateurs autorisés à accéder au réseau Wi-Fi.

Dans le dossier Users, on fait un click droit puis Nouveau groupe que l'on appellera **groupe-wifi**.

On va faire un click droit sur le groupe groupe-wifi puis aller dans propriétés. Dans l'onglet **Membres**, on sélectionne ajouter. On ajoute alors l'utilisateur util1-wifi.



L'utilisateur util1-wifi fait donc maintenant partie de groupe-wifi. ***On répétera la procédure autant de fois pour créer d'autres utilisateurs***.

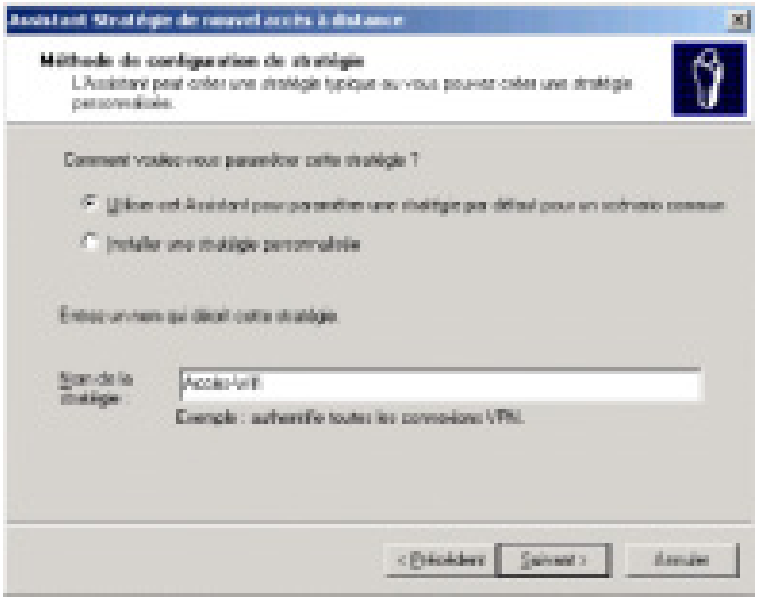
Maintenant on peut donc passer à la configuration du serveur Radius.

b- Configuration du serveur Radius

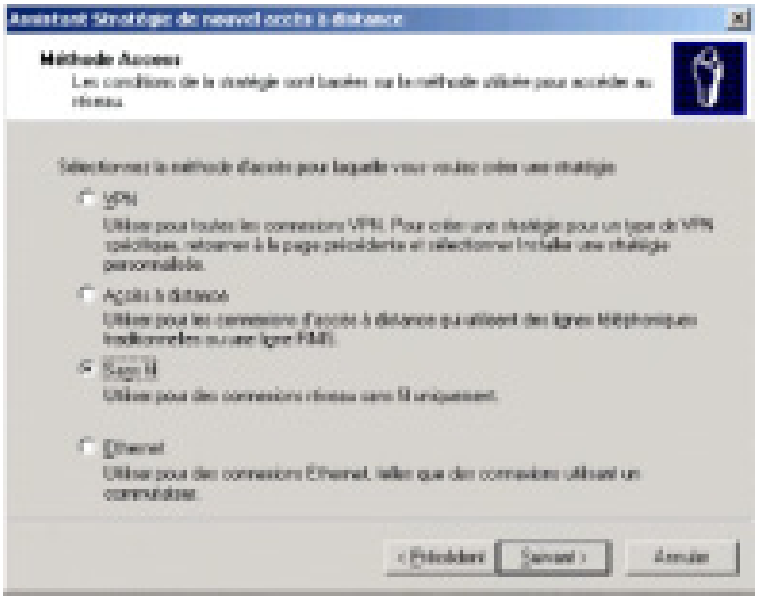
Tout d'abord on va dans le menu Démarrer puis Outils d'administration et enfin on sélectionne **Service d'authentification Internet**.

Dans le dossier **Stratégie d'accès distant**, on fait un click droit puis **Nouvelle stratégie d'accès distant**.

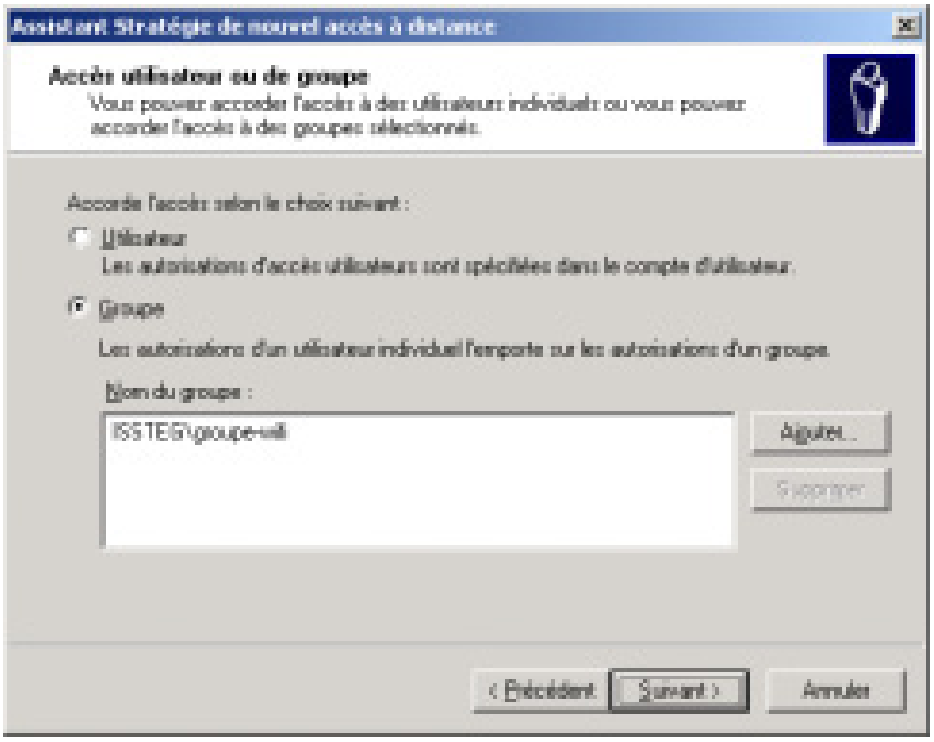
On **coche Utiliser cet assistant pour paramétrer une stratégie par défaut pour un scénario commun**. Puis on va entrer le nom de la nouvelle stratégie.



On valide par suivant puis on coche la méthode d'accès Sans fil.

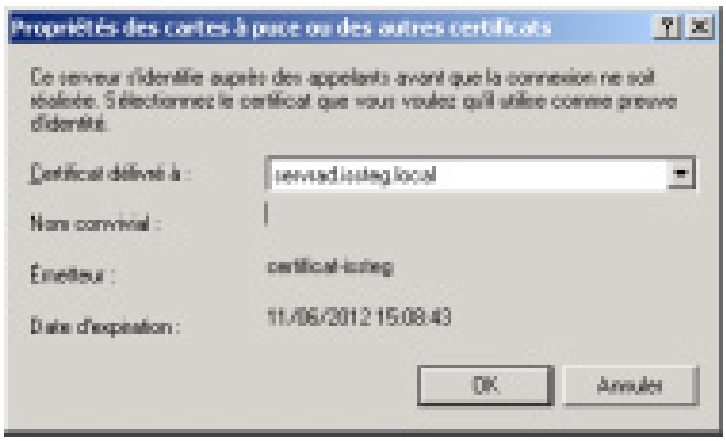


On continue en validant par suivant et on ajoute le groupe groupe-wifi à la liste d'accès.



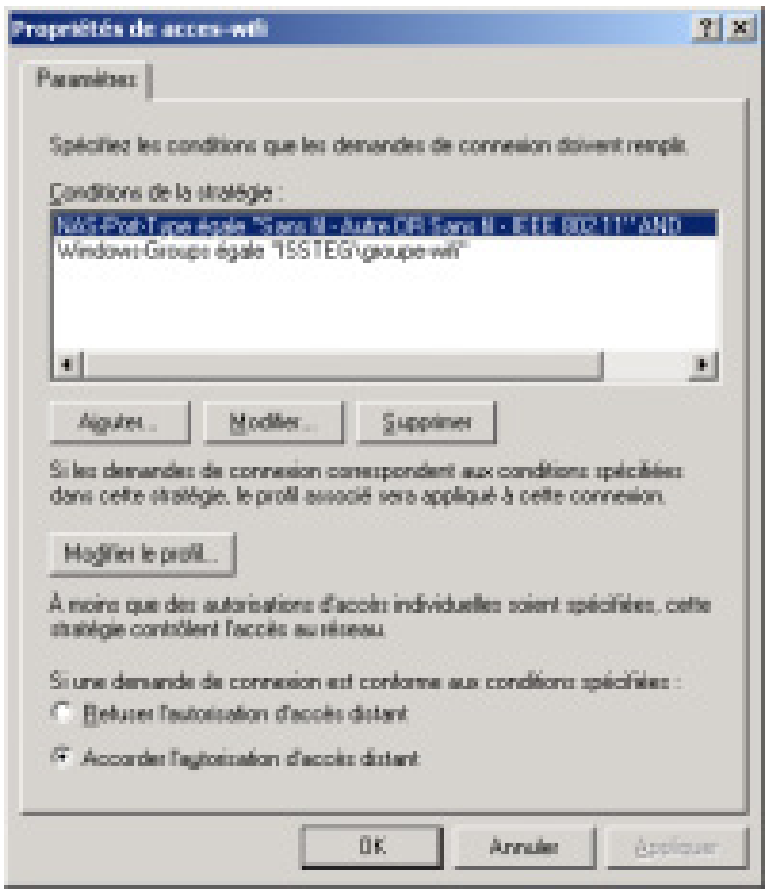
On clique sur Suivant puis on sélectionne **Carte à puce ou autre certificat**.

On sélectionne configurer pour vérifier qu'il s'agit bien du serveur sur lequel on vient d'installer l'autorité de certification racine. Dans notre cas, l'émetteur est **certificat-issteg** et le certificat est délivré à **issteg** (nom DNS du serveur).



On fini l'installation en cliquant sur suivant et terminer.

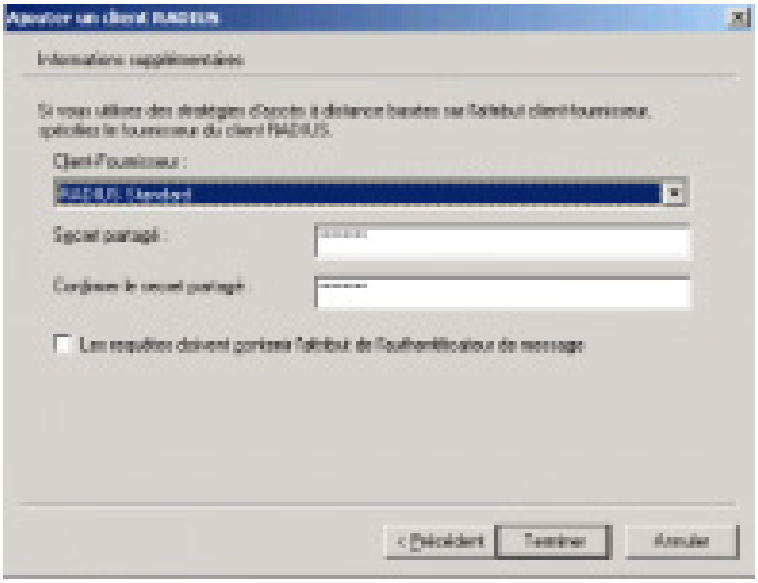
Nous allons maintenant vérifier les paramètres de la nouvelle stratégie. On fait un click droit sur la nouvelle stratégie Accès-Wifi puis propriétés. On vérifie que l'option **Accorder l'autorisation d'accès distant** est bien cochée.



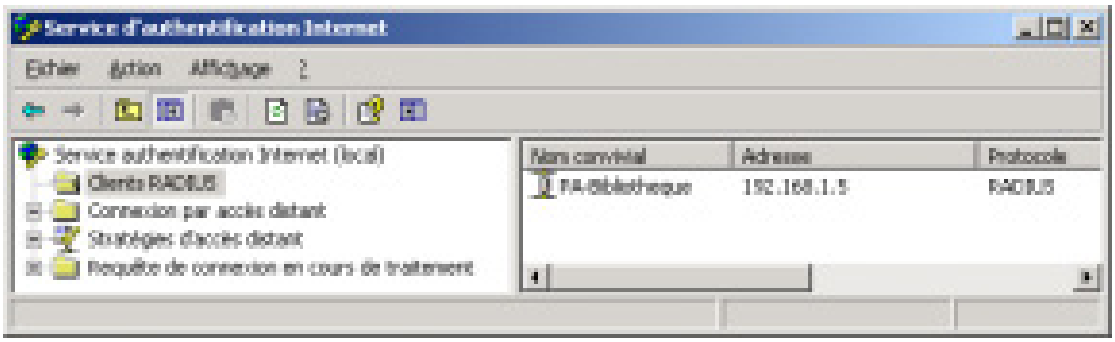
Maintenant, dans le dossier Client Radius on fait un click droit puis **ajouter un client RADIUS**.

Puis on entre un nom convivial qui sera celui de notre point d'accès WiFi ainsi que son adresse IP.

On choisi le nom **issteg-wifi** et le mot de passe : ******** et on valide par suivant puis on va définir le secret partagé entre le point d'accès et le serveur Radius. Dans notre cas nous utiliserons la marque de notre point d'accès.



Le point d'accès apparaît alors dans la liste des clients Radius.



La configuration du serveur Radius est maintenant terminée.

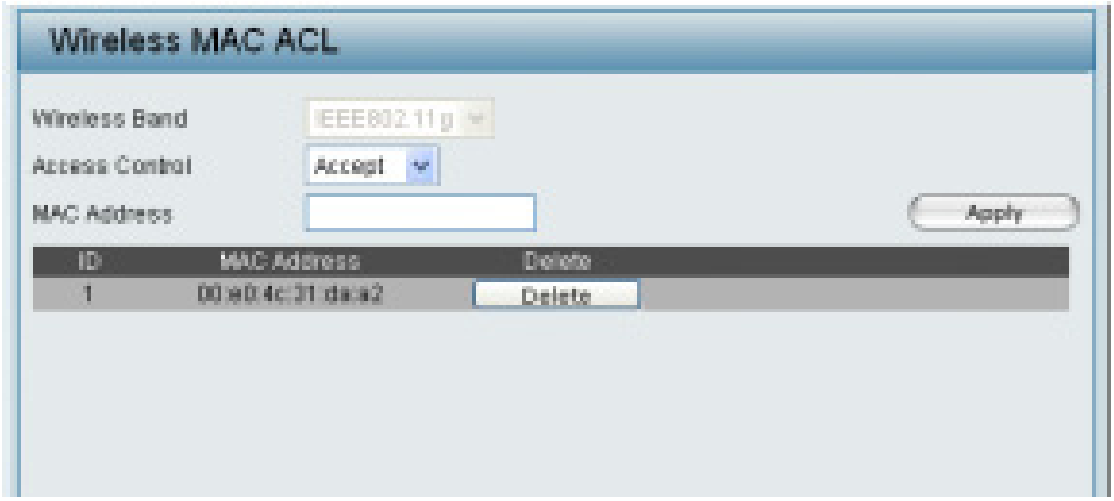
4- Installation et sécurisation du point d'accès wi-fi

On ouvre Internet Explorer sur une machine connectée sur un autre port du commutateur (dans ce cas c'est notre serveur) et on saisit l'adresse par défaut du point d'accès, **http://192.168.1.5**. Une fenêtre de connexion s'affiche. Alors, on entre notre login et notre mot de passe (ce login et ce mot de passe sont fournis avec l'équipement) puis on va dans le menu paramètres sans fil.

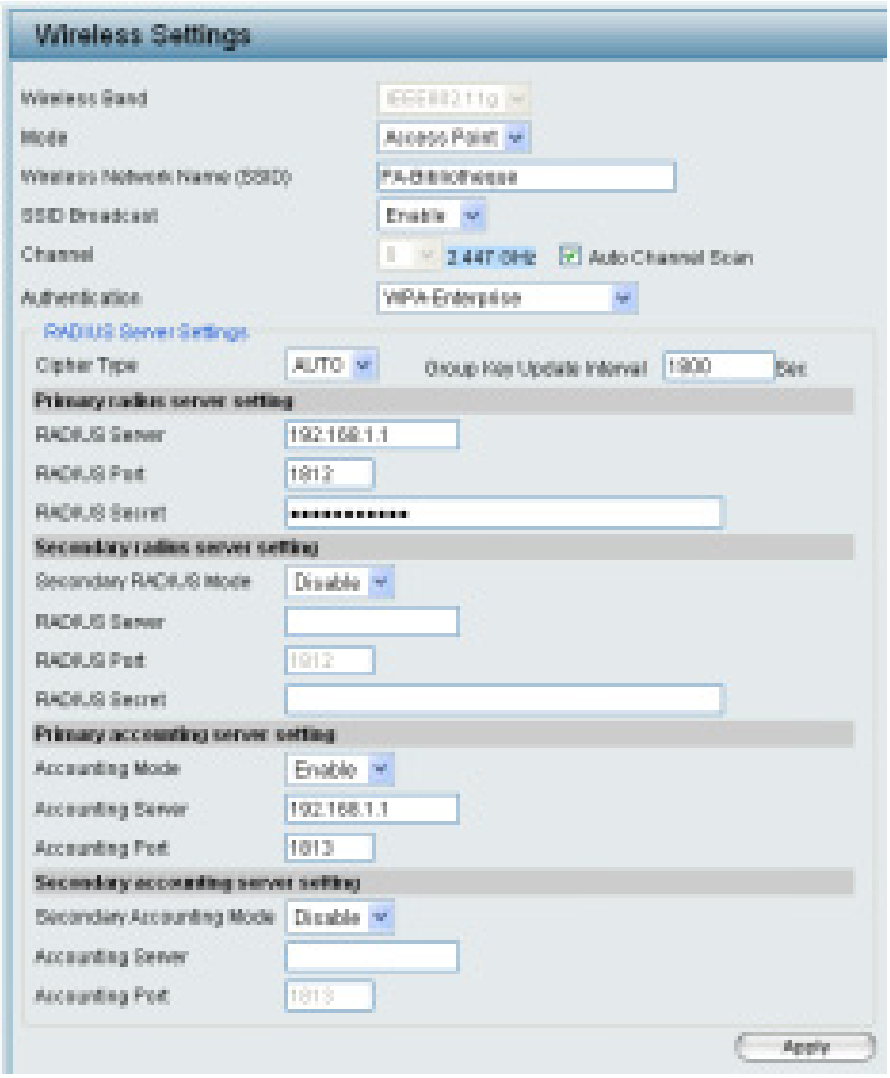
Première opération de sécurité : on désactive la diffusion du nom SSID. Puis on clique sur le bouton configuration de la liste d'accès.

Deuxième opération de sécurité : on change le mot de passe par défaut de l'AP et on en prend un qui soit compliqué.

Troisième opération de sécurité : on active le contrôle d'accès et on va à la section liste d'accès. Là, on entre les adresses MAC des clients autorisés à accéder au réseau Wi-Fi.



Enfin on choisit l'option de sécurité WPA-802.1X. On entre l'adresse IP de notre Serveur Radius et le port de communication (par défaut 1812 pour l'authentification et 1813 pour l'accounting). Puis on entre la clé partagée qu'on a saisie sur le serveur Radius.



La configuration du point d'accès est terminée, nous allons pouvoir passer à la configuration des clients d'accès Wi-Fi.

5- Configuration d'un client d'accès wi-fi

a- Installation du certificat auto signé du serveur d'authentification et du certificat d'un utilisateur

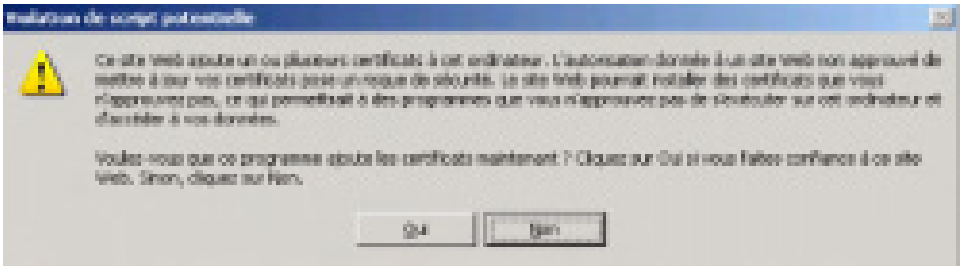
Tout d'abord on ouvre une session sous le nom de l'utilisateur qui recevra le certificat sur cette machine.

Puis dans un navigateur, on se connecte sur le serveur de l'autorité de certification : http:// "nom du serveur "/certsrv. Dans notre cas **http://192.168.1.1/certsrv.**

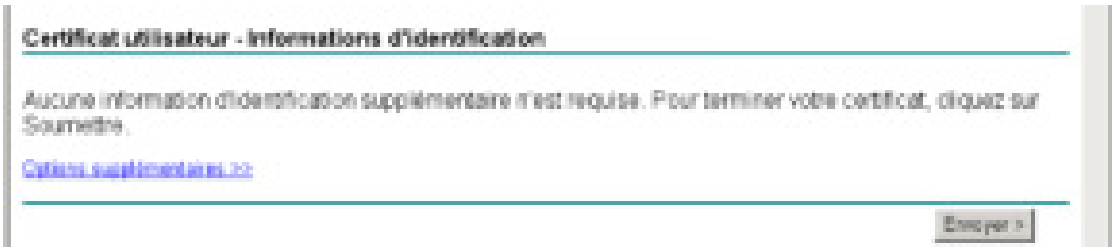
On entre le login et le mot de passe de l'utilisateur «util1-wifi» par exemple dans la fenêtre de connexion qui surgit.

A la page d'accueil, on clique sur **Télécharger un certificat d'autorité de certification, une chaine de certificats ou une liste de révocation de certificats** puis sur **Installer cette chaîne de certificats d'autorité de certification**.

Une fenêtre s'ouvre, on clique sur oui pour confirmer l'installation.



Puis on retourne à la page d'accueil et on va maintenant suivre le lien **demander un certificat**, puis le lien **certificat utilisateur** et enfin on clique sur le bouton envoyer.

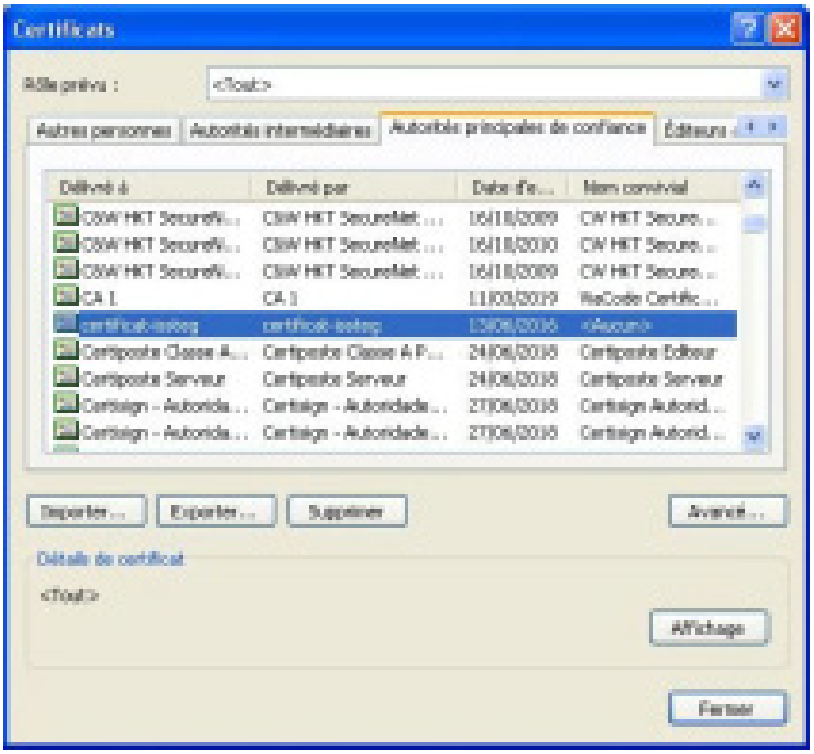


On confirme la demande de certificat en cliquant sur oui.

On clique sur installer ce certificat. Puis, sur oui on valide qu'on fait confiance à ce site et le certificat est installé.

Pour vérifier l'effectivité de ces paramètres, dans Internet Explorer on va dans le menu déroulant Outils puis Options Internet puis dans l'onglet contenu, enfin on clique sur certificats. On vérifie que le certificat pour l'utilisateur util1-wifi est bien présent.

On vérifie également que le serveur de certificat est bien présent dans la liste des autorités principales de confiance.

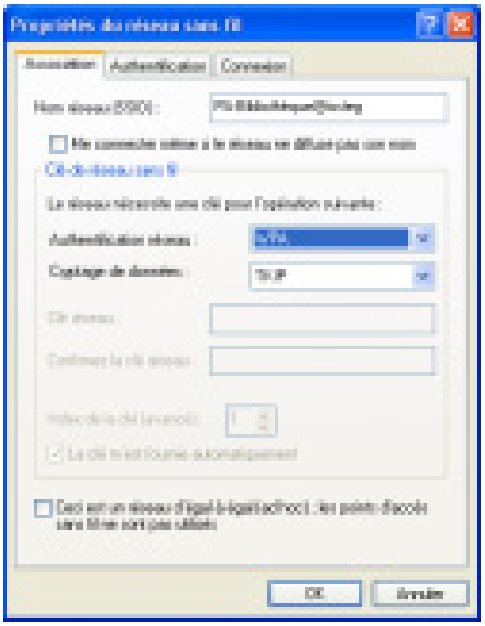


L'installation du certificat est maintenant terminée. Nous allons pouvoir passer à la configuration de la connexion réseau sans-fil.

b- Configuration de la connexion réseau sans-fil

On va dans Panneau de Configuration puis Connexions réseaux.

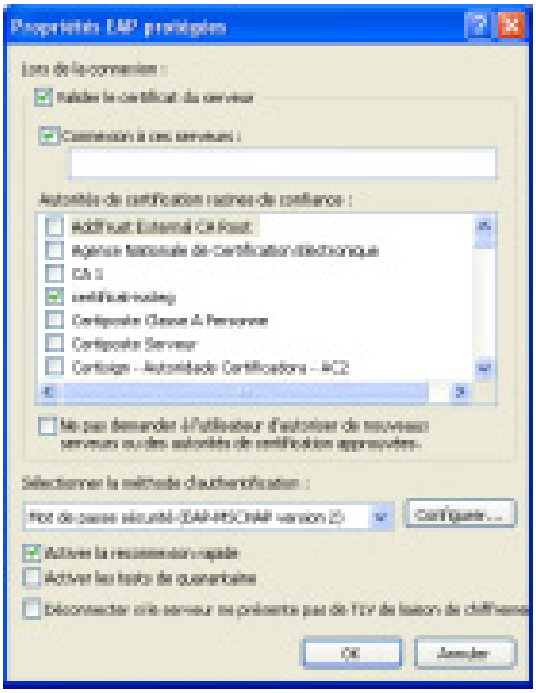
On fait un click droit sur Connexion réseaux sans-fil puis on entre dans les propriétés. Dans l'onglet Configuration réseaux sans-fil on clique sur ajouter. On entre le nom de notre réseau et on choisit la méthode d'authentification de type WPA et un cryptage de type TKIP.



Dans l'onglet authentification on sélectionne Activer l'authentification IEEE 802.1X pour ce réseau et on clique sur propriétés du type EAP.

On décoche l'option connexion à ces serveurs.

Puis on sélectionne notre serveur de certificat dans la liste des autorités de certification racine de confiance.



La connexion est configurée et opérationnelle sur cette machine, on peut donc désormais se connecter au réseau sans-fil dessus. On va répéter la procédure pour toutes les autres machines clientes tournant sous Windows XP.

II. OBSERVATIONS ET TESTS

Comme vous l'avez sûrement remarqué, la connexion au réseau Wi-Fi de l'ISSTEG s'effectue lors d'une ouverture de session sur le domaine issteg.

Ainsi, lorsqu'un utilisateur souhaite accéder au réseau, il devra ouvrir une session sur le réseau avec son compte du domaine qui lui aura été fourni préalablement par l'administrateur du réseau. Si tout a été convenablement configuré sur la machine utilisée, la connexion au réseau se fera de manière transparente. Si la connexion ne fonctionne pas, il faudra s'adresser au service technique. Ainsi, toutes les machines nécessitant se connecter au réseau devront automatiquement passer par le service technique pour être configurées et les utilisateurs aussi afin d'obtenir les informations sur leurs comptes d'accès.

Par défaut, l'adaptateur sans fil Wi-Fi du poste client gère les déconnexions après un certain temps d'inactivité. Bien plus la fermeture de session ou l'extinction du poste client réalise la déconnexion du réseau. Nous pensons que ceci permettra de renforcer la sécurité de notre réseau sans fil Wi-Fi.

Pour les machines disposant en plus de l'adaptateur Wi-Fi une carte Ethernet, la configuration IP de cette dernière devra être similaire avec

celle de l'adaptateur Wi-Fi afin que le passage du sans fil au filaire se fasse de manière transparente. Et notons ici que la connexion au réseau se fera tout naturellement au démarrage de la machine sans passer par une authentification préalable.

Nous allons maintenant tester si les machines arrivent à communiquer entre elles. La commande utilisée est PING (Packet INternet Groper), elle sert à vérifier la connectivité IP à un autre ordinateur en envoyant des messages Requête d'écho ICMP (Internet Control Message Protocol). Si tout est bien configuré on reçoit des réponses positives signifiant que les deux machines arrivent à communiquer entre elles.

Et voila maintenant que le réseau sans fil Wi-Fi a été installé, et tous les tests sont effectues avec succès et on espère avoir établi une solution plus sure, plus efficace et surtout plus sécurisée.

CONCLUSION

Ainsi, nous avons tout au long de ce stage mis en place une infrastructure Wi-Fi espérant qu'elle soit la plus sécurisée possible tout en restant compatible avec les différentes technologies existantes.

Notons cependant que si le réseau Wi-Fi présente des avantages en confort et en utilisation qui sont considérables, il n'est pas adapté à de lourdes charges, et il faut savoir que les coûts économisés en évitant un câblage Ethernet pour les postes des utilisateurs peuvent être dépassés par d'autres coûts auxquels on n'a pas forcément pensé à l'origine.

En pratique, les réseaux Wi-Fi sont performants en mode client-serveur avec des échanges courts (navigation Internet par exemple), ce qui explique leur succès auprès des particuliers.

ANNEXES

Annexe 1 : Sécurité des réseaux Wi-Fi

Les réseaux sans fil sont non sécurisés par défaut !

Sans faire trop compliqué, beaucoup de points d'accès possèdent un serveur DHCP qui permet à tout client d'obtenir un accès sur ce dernier. Un serveur DHCP permet à un ordinateur d'obtenir tous les paramètres nécessaires pour communiquer sur le réseau, comme l'adresse IP, la passerelle pour se connecter à internet, les serveurs de résolution des noms de domaine, etc.. Or ce dernier est trop souvent activé par défaut sur les points d'accès : grâce à cette caractéristique toute personne passant à portée radio de votre point d'accès pourra se faire attribuer une IP sur ce dernier. Les protections supplémentaires comme le filtrage d'adresse MAC (unique pour chaque carte réseau) et le cryptage WEP intégré dans pratiquement tous les matériels wifi ne seront que des protections en plus mais sachez qu'elles sont très facilement contournables. En effet la clef WEP ne change pas régulièrement, donc il suffit pour un ordinateur voulant se connecter sur votre réseau d'écouter les transmissions de vos postes pour obtenir, après un certains nombre de données échangées, la clef WEP car les données se cryptent toujours de la même manière avec la même clef. Une norme supérieure d'encodage des données est en train d'être mise en place pour remédier à ce problème.

"Je sais qui vous êtes" : Lorsque vous demandez à votre matériel équipé d'une carte wifi de trouver les réseaux disponibles il va faire référence aux SSID, qui représentent l'identifiant réseau. A l'inverse si vous connaissez une adresse MAC du point d'accès ou d'une carte wifi vous saurez immédiatement de quel matériel il s'agit.

Constructeur	**SSID par défaut**	**MAC ID**
Apple	Airport	00:30:65
Cisco Aironet	tsunami	00:40:96
DLINK	…….	……

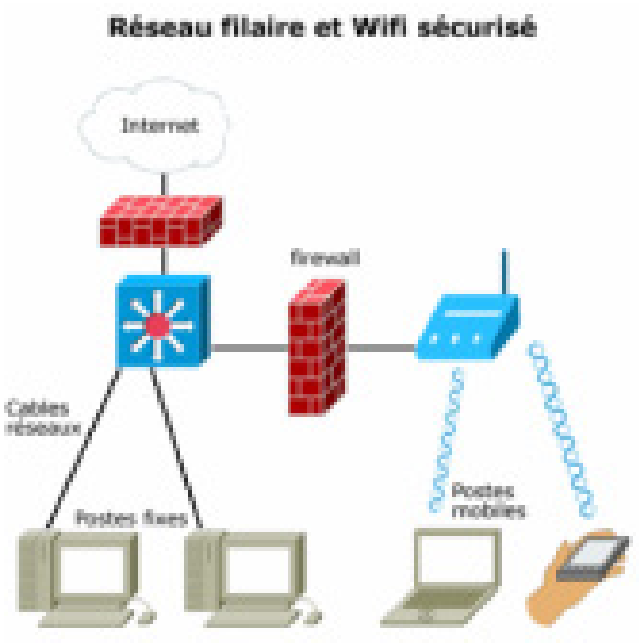
Voici quelques conseils pour sécuriser un peu plus son réseau sans fils :

- Modifiez le nom SSID par défaut.
- Désactivez SSID Broadcasts (Diffusion du nom SSID).
- Modifiez le mot de passe par défaut du compte de l'administrateur
- Activez MAC Address Filtering (Filtrage des adresses MAC).
- Modifiez régulièrement le nom SSID.
- Activez le cryptage WEP. (L'activation du WEP est un plus mais ralentit le débit d'information : temps de cryptage - décryptage).
- Modifiez les clés de cryptage WEP régulièrement.

Pour les connaisseurs ou experts en réseaux et surtout pour les entreprises:

- Installez un firewall comme si le point d'accès était une connexion internet.
- Ce firewall sera le serveur ipsec (VPN) des clients sans fils.
- Faire l'authentification grâce à un serveur LDAP, Radius.

Chacun est libre de modifier ces règles en ajoutant des couches supplémentaires. Sachez que le futur protocole IP ipv6 contient dans ses paquets la sécurisation ipsec. L'ipv6 peut être utilisé en wifi si les clients gèrent l'ipv6, actuellement tous les Linux, Unix ont une pile ipv6 fonctionnelle, sur windows 2000 et XP l'ipv6 est activable et utilisable mais sera proposé par défaut dans les prochaines versions.



Un réseau wifi "sécurisé" peut se shématiser comme ci-dessus. On considère içi que tout le réseau Wifi est étranger au réseau local, au même titre qu'internet. L'utilisation d'un parefeu (firewall) comme pour la connexion internet, permet de filtrer les adresses MAC associé à des adresses IP fixes. Dans le cas du VPN, le firewall ou un serveur derrière ce dernier fait office de terminal VPN. Certains points d'accès proposent des "petits" firewall permettant de faire un filtrage de plus sur les clients de votre réseau.

La sécurisation d'un réseau qu'il soit filaire ou sans fils est possible par de nombreux moyens matériels et/ou logiciels. Son choix dépend de l'utilisation que vous voulez faire de votre réseau et des moyens dont vous disposez.

Annexe2 : Généralités sur le protocole RADIUS

L'authentification est l'opération par laquelle le destinataire et/ou l'émetteur d'un message s'assure (nt) de l'identité de son interlocuteur. L'authentification est une phase cruciale pour la sécurisation de la communication. Les utilisateurs doivent pouvoir prouver leur identité à leurs partenaires de communication et doivent également pouvoir vérifier l'identité des autres utilisateurs. L'authentification de l'identité sur un réseau est une opération complexe, car les parties qui communiquent ne se rencontrent pas physiquement lors de la communication. Un utilisateur malveillant peut ainsi intercepter des messages ou emprunter l'identité d'une autre personne ou entité.

Le protocole RADIUS (*Remote Authentication Dial-In User Service)* en français « service d'authentification distante des utilisateurs d'accès à distance », mis au point initialement par la société Livingston, est un protocole d'authentification standard, défini par les RFC 2865 (pour l'authentification) et 2866 (pour la comptabilité).

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau en utilisant le protocole UDP et les ports 1812 et 1813. Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, Active Directory, annuaire LDAP, etc.) et 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 chiffrée et authentifiée grâce à un secret partagé.

Le scénario du principe de fonctionnement est le suivant :

- ✓ 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 :

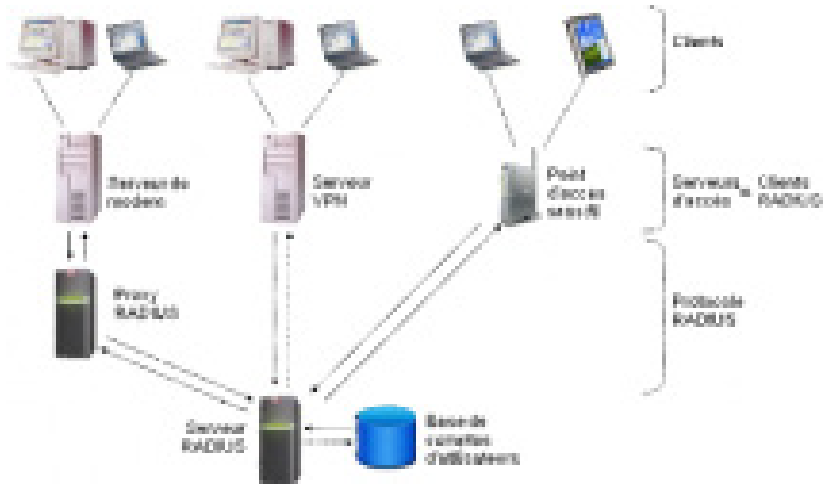
o **ACCEPT** : l'identification a réussi ;

o **REJECT** : l'identification a échoué ;

o CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « *challenge* ») ;

o CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

Suite à cette phase dit d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.



Il est à noter que le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS. L'en-tête du paquet RADIUS comporte 5 champs:

1. Code : Définit le type de trame (acceptation, rejet, challenges, requête)
2. Identifier : Associe les réponses reçues aux requêtes envoyées.
3. Length : Champ longueur.
4. Authentificator : Champ d'authentification comprenant les éléments nécessaires.
5. Attributes : Ensemble de couples (attribut, valeur).

En-tête d'un paquet RADIUS

Annexe3 : Glossaire des principaux sigles et acronymes utilisés

Terme	Définition
Adresse MAC (Media Access Control)	Adresse matérielle d'un périphérique raccordé à un support de réseau partagé.
AES (Advanced Encryption Standard)	Technique de cryptage de données par bloc de 128 bits symétrique.
Bande ISM (Intermediate Service Module)	Bande radio utilisée dans les transmissions de mise en réseau sans fil.
Bit (chiffre binaire)	Plus petite unité d'information d'une machine.
CSMA/CA (Accès multiple par détection de porteur./Autorité de certification)	Méthode de transfert de données utilisée pour empêcher les collisions de données.
DHCP (Dynamic Host Configuration Protocol)	Protocole qui permet à un périphérique d'un réseau local, le serveur DHCP, d'affecter des adresses IP temporaires à d'autres périphériques réseau, généralement des ordinateurs.
DNS (serveur de nom de domaine)	Adresse IP du serveur de votre ISP, qui traduit les noms des sites Web en adresses IP.
Domaine	Nom spécifique d'un réseau d'ordinateurs.
EAP (Extensible Authentication Protocol)	Protocole d'authentification général utilisé pour contrôler l'accès au réseau. De nombreuses méthodes d'authentification fonctionnent avec cette infrastructure.
EAP-PEAP (Extensible Authentication Protocol-Protected Extensible Authentication Protocol)	Méthode d'authentification mutuelle qui utilise des certificats numériques en plus d'un autre système, tels que des mots de passe.
EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)	Méthode d'authentification mutuelle qui utilise des certificats numériques.
Étalement du spectre	Technique de fréquence radio large bande utilisée pour une transmission de données plus fiable et sécurisée.
IEEE (The Institute of Electrical and Electronics Engineers)	Institut indépendant qui développe des normes de mise en réseau.
Infrastructure	Matériel informatique et de mise en réseau actuellement installé.
ISP (fournisseur de services Internet)	Société qui procure un accès à Internet.
LAN (réseau local)	Ordinateurs et produits de mise en réseau qui constituent le réseau à votre domicile ou votre bureau.
Mbit/s (Mégabits par seconde)	Un million de bits par second ; unité de mesure pour la transmission de données.
NAT (traduction d'adresses réseau)	La technologie NAT traduit des adresses IP du réseau local en adresses IP différentes pour Internet.
NNTP (Network News Transfer Protocol)	Protocole utilisé pour se connecter à des groupes Usenet sur Internet.
OFDM (multiplexage fréquentiel orthogonal)	Type de technologie de modulation qui sépare le flux de données en un nombre de flux de données bas débit, qui sont ensuite transmises en parallèle.
PoE (Power over Ethernet)	Technologie permettant à un câble réseau Ethernet de

	fournir des données et l'alimentation électrique.
RADIUS (Remote Authentication Dial-In User Service)	Protocole qui utilise un serveur d'authentification pour contrôler l'accès au réseau.
SNMP (Simple Network Management Protocol)	Protocole de contrôle et de surveillance du réseau largement utilisé.
SSID (Service Set IDentifier)	Nom de votre réseau sans fil.
TCP/IP (Transmission Control Protocol/Internet Protocol)	Protocole réseau de transmission de données qui exige un accusé de réception du destinataire des données envoyées.
TKIP (Temporal Key Integrity Protocol)	Protocole de cryptage sans fil qui modifie périodiquement la clé de cryptage, la rendant plus difficile à décoder.
TLS (Transport Layer Security)	Protocole qui garantie la protection des informations confidentielles et l'intégrité des données entre les applications client/serveur qui communiquent sur Internet.
UDP (User Datagram Protocol)	Protocole réseau de transmission de données qui n'exige aucun accusé de réception du destinataire des données envoyées.
URL (Uniform Resource Locator)	Adresse d'un fichier qui se trouve sur Internet.
WEP (Wired Equivalency Protocol)	WEP est un protocole de sécurité pour les réseaux sans fil. WEP offre un niveau de sécurité de base mais satisfaisant pour la transmission de données sans fil.
WLAN (réseau local sans fil)	Groupe d'ordinateurs et de périphériques associés qui communiquent sans fil entre eux.
WPA (Wi-Fi Protected Access)	Protocole de sécurité pour les réseaux sans fil qui repose sur les fondations de base du protocole WEP. Il sécurise la transmission de données sans fil en utilisant une clé similaire à la clé WEP, mais sa force est que cette clé change dynamiquement. Il est donc plus difficile pour un pirate de la découvrir et d'accéder au réseau.

Annexe 4 : Guide d'installation du PA DWL-3200AP

Configuration requise

Configuration minimale requise :

- Lecteur de CD-ROM
- Ordinateur équipé du système d'exploitation Windows, Macintosh ou Linux
- Adaptateur Ethernet installé
- Internet Explorer version 6.0 ou Netscape Navigator version 7.0 ou supérieure

Contenu du coffret

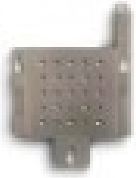
DWL-3200AP *Air*Premier™ D-Link
Point d'accès géré sans fil

Cordon d'alimentation

Unité de base PoE
(Power over Ethernet)

Câble Ethernet

CD-ROM contenant le manuel



Plaque de montage

Adaptateur d'alimentation
48V, 0,4A CC

Le fait d'utiliser un adaptateur d'alimentation de tension nominale différente risque d'endommager le produit et d'en annuler la garantie.

Configuration requise Guide d'installation du DWL-3200AP

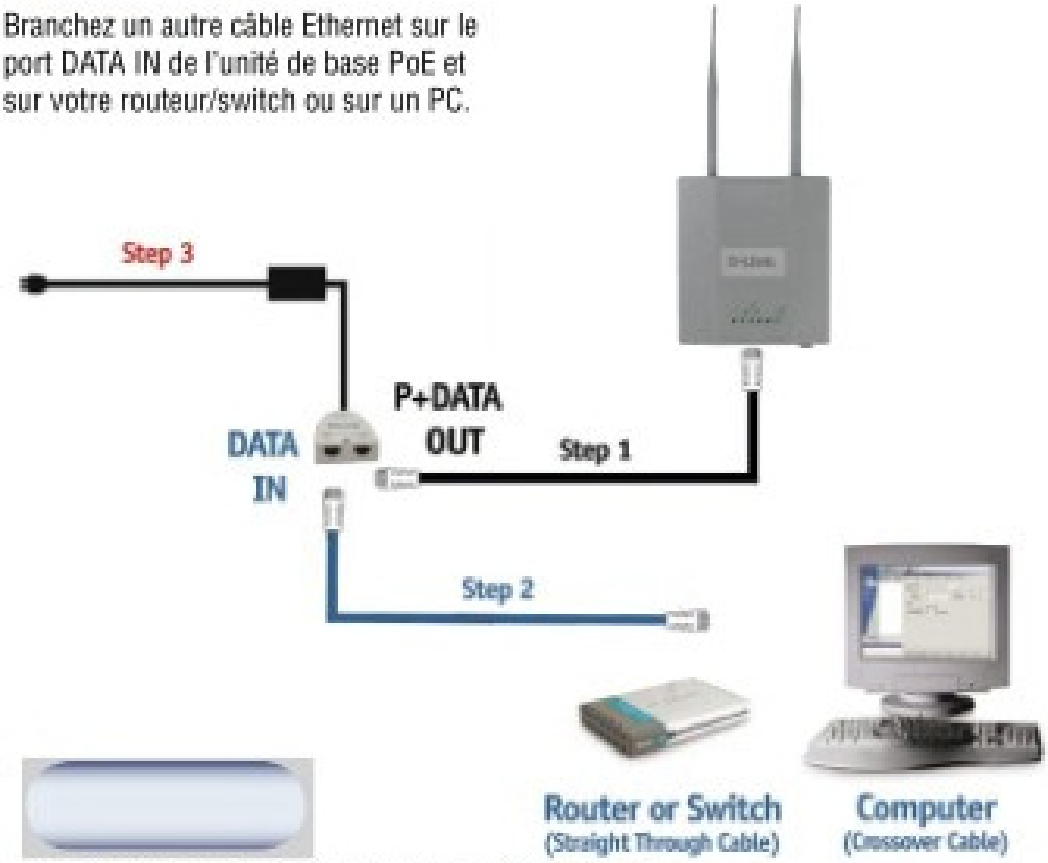
Installation du matériel

Etape 1

Branchez une extrémité d'un câble Ethernet (contenu dans votre coffret) sur le port LAN du DWL-3200AP, et l'autre extrémité de ce câble sur le port marqué P+DATA OUT sur l'unité de base PoE.

Etape 2

Branchez un autre câble Ethernet sur le port DATA IN de l'unité de base PoE et sur votre routeur/switch ou sur un PC.



Branchez l'adaptateur d'alimentation sur le connecteur marqué POWER IN sur l'unité de base PoE. Branchez le cordon d'alimentation sur l'adaptateur d'alimentation et sur une prise murale.

2

L'Assistant de configuration Guide d'installation du DWL-3200AP

Les écrans suivants apparaissent.

Cliquez sur « Next » (Suivant)

Etape 1 – Définition du nouveau mot de passe. Vous avez la possibilité de définir un mot de passe.

Cliquez sur « Next » (Suivant)

Pour les réseaux **802.11g**, veuillez procéder comme suit :

Etape 2 – Etablissement de la connexion LAN sans fil.

Par défaut, le **SSID** du DWL-3200AP est initialisé à « **default** » **(valeur par défaut)** et le « **Channel** » **(canal)** est initialisé à **6**.

Cliquez sur « Next » (Suivant)

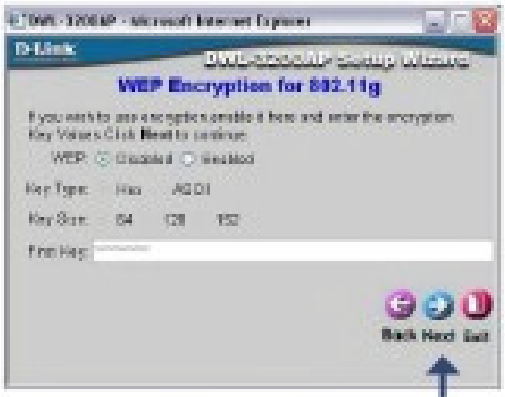
4

Guide d'installation du DWL-3200AP L'Assistant de configuration

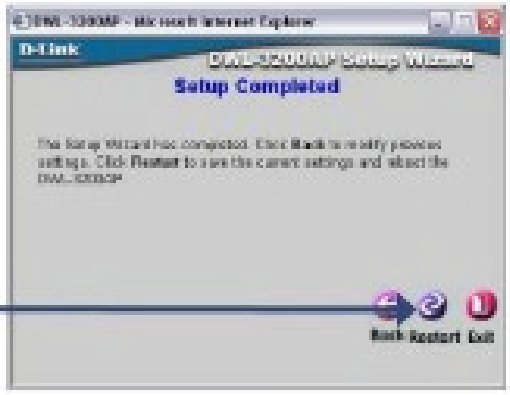
Pour les réseaux **802.11g**, veuillez continuer comme suit :

Etape 3 - Cryptage

Le DWL-3200AP permet trois niveaux de cryptage sans fil : 64, 128 et 152 bits, avec clé hexadécimale ou ASCII. Par défaut, le cryptage est désactivé. Vous pouvez modifier vos paramètres de cryptage, ce qui vous permet de renforcer la sécurité de vos communications sans fil.



Cliquez sur « Next » (Suivant)



Cliquez sur « Restart » (Redémarrer)

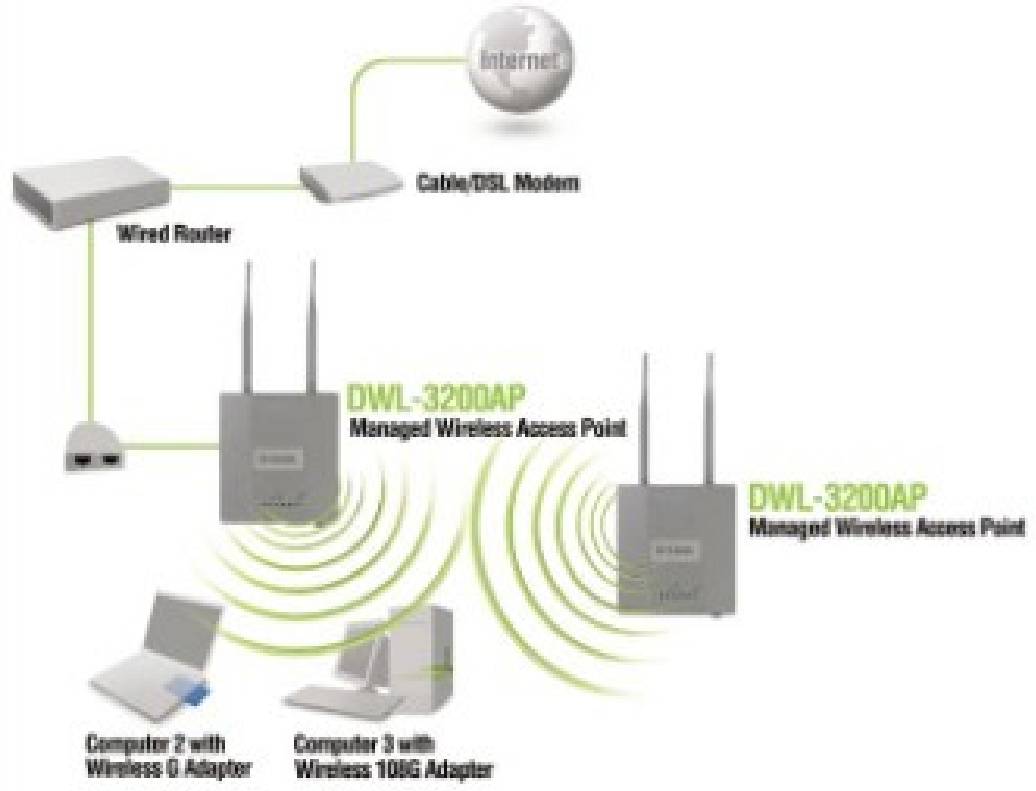
Votre installation est terminée !

5

L'Assistant de configuration Guide d'installation du DWL-3200AP

Votre installation est terminée !

Une fois que vous avez terminé toute la procédure décrite dans ce Guide d'Installation Rapide, votre réseau connecté doit avoir l'aspect suivant :



6

BIBLIOGRAPHIE

http://fr.wikipedia.org/

http://www.commentcamarche.net/

http://www.isstegb.rnu.tn/

http://www.dlink.fr/