

SOMMAIRE

Mission 4 : Wifi.....	1
PRÉSENTATION du TP :.....	1
MÉTHODE :.....	2
Partie A : Configuration de la borne wifi.....	2
1) Configuration de Base de la borne wifi	2
2) Configuration du SSID	3
3) Configuration de la sécurité WPA personnel	4
4) Configuration de la sécurité WPA professionnel.....	5
Partie B : Mise en place du serveur Radius	6

PRÉSENTATION DU TP :

La mission 4 consiste à mettre en place pour chaque ligue un réseau WiFi dans un premier temps par clef partagée (WEP, WPA2-PSK), puis dans un second temps nous allons configurer une authentification utilisateur avec la borne WiFi et un serveur radius en configurant la borne en WPA Entreprise

Un serveur RADIUS est un serveur chargé d'authentifier un utilisateur, il utilise le protocole radius général pour pouvoir s'adapter a un grand nombre d'appareils si on lui demande d'authentifier un utilisateur.

MÉTHODE :

PARTIE A : CONFIGURATION DE LA BORNE WIFI

1) CONFIGURATION DE BASE DE LA BORNE WIFI

Après avoir connecté la borne WiFi sur un pc en « local », il faut aller sur l'interface web de la borne Cisco en tapant l'adresse URL qui lui a été confiée par défaut, c'est-à-dire 192.168.1.245

Il faut entrer « admin » en login puis « admin » en mot de passe.

Maintenant nous allons changer l'adresse IP de la borne pour qu'elle soit conforme avec notre réseau de ligue, c'est-à-dire en 172.16.32.211. N'oublions pas bien évidemment de mettre la passerelle utilisée par notre réseau.

The screenshot shows the 'Basic Setup' configuration page for a Cisco device. It is divided into three main sections: Device Setup, Network Setup, and IPv6.

- Device Setup:** Host Name and Device Name are both set to 'BorneWifi'.
- Network Setup:** IP Settings are set to 'Static IP Address'.
 - IPv4:** Local IP Address is 172.16.32.211, Subnet Mask is 255.255.255.0, Default Gateway is 172.16.32.254, Primary DNS is 0.0.0.0, and Secondary DNS is 0.0.0.0.
- IPv6:** IPv6 is set to 'Disabled'.

On note bien l'adresse IP de notre serveur NTP, ici 172.16.32.210 en cochant « enabled ».

The screenshot shows the 'Time' configuration page. The 'Manually' option is selected. The date is set to Jan 1, 2008, and the time is 0:00. The 'Automatically' option is unselected. The time zone is '(GMT+01:00) Brussels, Copenhagen, Madrid, Paris'. The 'Automatically adjust clock for daylight saving changes' checkbox is unselected. The 'User Defined NTP Server' is set to 'Enabled'. The NTP Server IP is 172.16.32.220. The current time is 2013/01/10 Thu 16:42:17 (+01:00).

2) CONFIGURATION DU SSID

Dans les options avancées, nous changeons le nom de notre SSID par notre ligue propre soit « liguebadminton », nous rendons le broadcast disponible « Enabled ».

The screenshot shows the 'Wireless' configuration page. The 'Basic Settings' tab is selected. The 'Wireless Network Mode' is set to 'B/G/N-Mixed' and the 'Wireless Channel' is set to 'Auto'. The SSID configuration table is as follows:

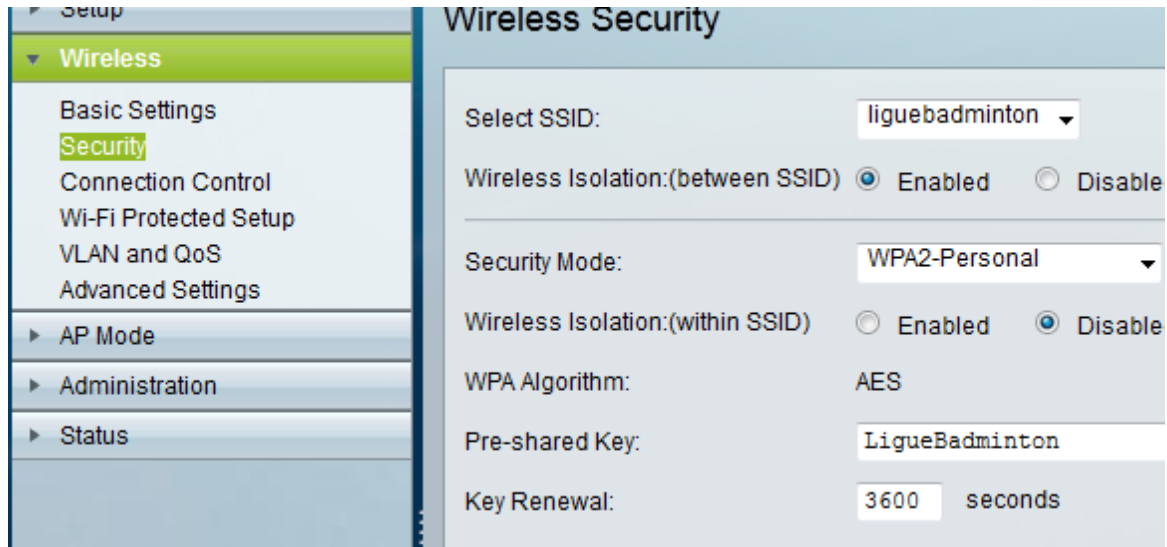
SSID	SSID Name	SSID Broadcast
SSID 1:	liguebadminton	Enabled
SSID 2:		Disabled
SSID 3:		Disabled
SSID 4:		Disabled

Buttons for 'Save' and 'Cancel' are visible at the bottom.

3) CONFIGURATION DE LA SECURITE WPA PERSONNEL

Au niveau de la sécurité, nous choisissons le mode WPA2-personal.

La clé partagée sera « LigueBadminton ».



Selectionnons notre SSID et passons en connexion Local.



Voilà, si nous branchons la borne nous l'avons bien configurée pour fonctionner avec une clé partager WPA2

Maintenant, nous configurons la borne pour utiliser un serveur radius qui va authentifier les utilisateurs qui se connecte à la borne WiFi avec un serveur RADIUS.

4) CONFIGURATION DE LA SECURITE WPA PROFESSIONNEL

Au niveau de la sécurité, choisissons le mode WPA2-Entreprise.

Dans Primary RADIUS server : on met l'adresse du serveur Radius

Et dans, Primary Shared Secret : on met une phrase (il faudra mettre la même dans le serveur radius)

The screenshot shows the 'Wireless Security' configuration page. On the left is a navigation menu with 'Wireless' expanded to show 'Security' selected. The main area contains the following settings:

- Select SSID: Wifi-GCR
- Wireless Isolation:(between SSID) Enabled Disabled
- Security Mode: WPA2-Enterprise Mixed
- Wireless Isolation:(within SSID) Enabled Disabled
- Primary RADIUS Server: 172 . 16 . 128 . 200
- Primary RADIUS Server Port: 1812
- Primary Shared Secret: [Redacted]
- Backup RADIUS Server: 0 . 0 . 0 . 0
- Backup RADIUS Server Port: 1812
- Backup Shared Secret: [Redacted]
- WPA Algorithm: TKIP or AES
- Key Renewal Timeout: 3600 seconds

At the bottom are 'Save' and 'Cancel' buttons.

PARTIE B : MISE EN PLACE DU SERVEUR RADIUS

Dans Windows Server 2008, nous allons installer le service d'authentification Internet qui a comme fonctionnalités RADIUS. Pour cela il vous faut aller dans le gestionnaire de serveur et dans "Ajouter un rôle" afin de sélectionner "Stratégie réseau et services d'accès" ensuite cliquer sur "Suivant".



Sélectionnez "Serveur NPS (Network Policy Server)" et "HCAP (Host Credential Authorization Protocol)". Cliquez sur "Suivant", cliquer sur suivant,

Assistant Ajout de rôles

Sélectionner les services de rôle

Avant de commencer
Rôles de serveurs
Stratégie et accès réseau
Services de rôle
Confirmation
État d'avancement
Résultats

Sélectionner les services de rôle à installer pour Services de stratégie et d'accès réseau :

Services de rôle :

- Serveur NPS (Network Policy Server)
- Services Routage et accès distant
 - Service d'accès à distance
 - Routage
- Autorité HRA (Health Registration Authority)
- HCAP (Host Credential Authorization Protocol)

Description :

[Le protocole HCAP \(Host Credential Authorization Protocol\) permet d'intégrer votre solution de protection d'accès réseau \(NAP\) Microsoft avec le contrôle d'accès réseau Cisco. Lorsque vous déployez HCAP avec le serveur NPS \(Network Policy Server\) et la protection d'accès réseau \(NAP\), le serveur NPS peut effectuer l'autorisation de clients de contrôle d'accès réseau Cisco.](#)

[En savoir plus sur les services de rôle](#)

Puis cliquez sur "Installer".

Assistant Ajout de rôles

Confirmer les sélections pour l'installation

Avant de commencer
Rôles de serveurs
Stratégie et accès réseau
Services de rôle
Confirmation
État d'avancement
Résultats

Pour installer les rôles, les services de rôle ou les fonctionnalités suivants, cliquez sur Installer.

1 message d'information ci-dessous

Il est possible que ce serveur doive être redémarré à la fin de l'installation.

Services de stratégie et d'accès réseau

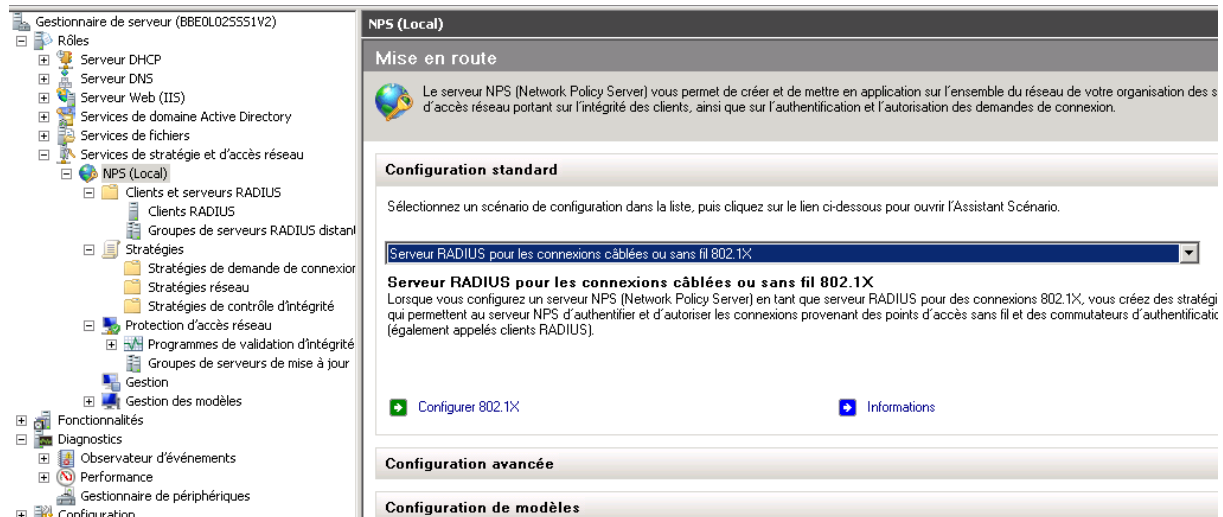
- Serveur NPS (Network Policy Server)**
- HCAP (Host Credential Authorization Protocol)**

[Imprimer, envoyer ou enregistrer cette information](#)

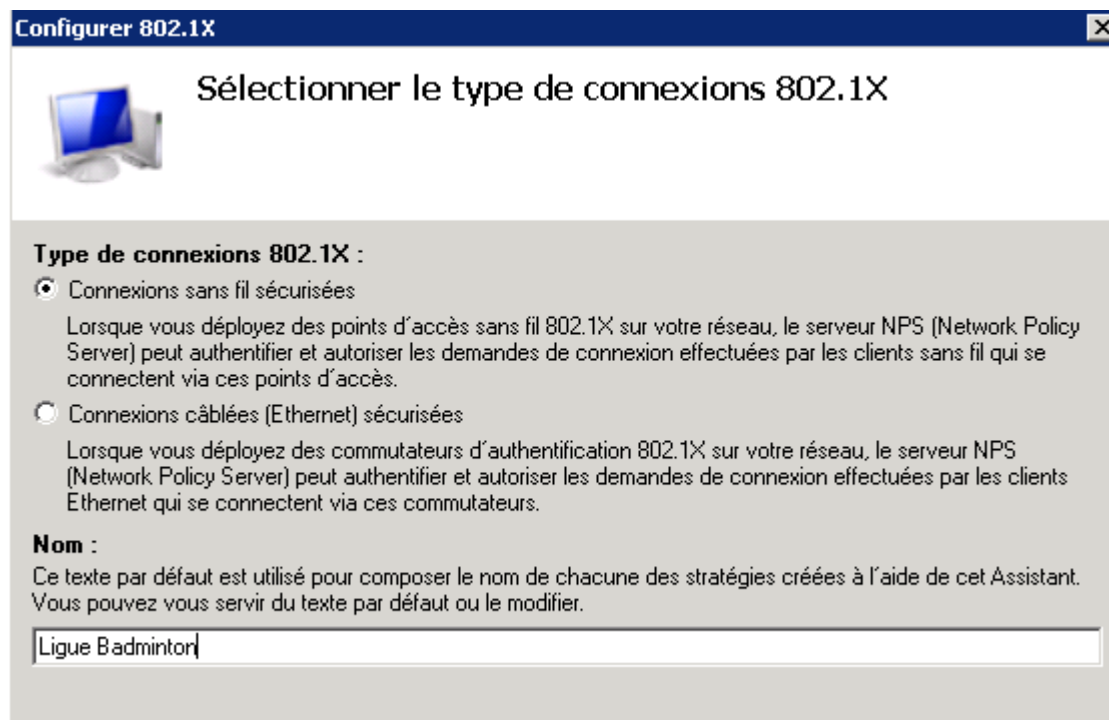
L'installation prendra quelques minutes.

Maintenant que le NPS est installé, allez dans l'arborescence et sélectionnez "NPS (Local)" ensuite dans l'assistant d'installation, "configuration standard" faites dérouler le menu et sélectionner le "serveur RADIUS pour les connexions câblées ou sans fil 802.1X".


Cliquez sur "Configurer 802.1X".



"Sélectionner le type de connexions 802.1X", sélectionnez "Connexions sans fil sécurisées", changer le Nom comme vous le souhaitez, moi j'ai choisi "Ligue Badminton" et cliquez sur "Suivant".



Maintenant vous cliquez sur "Ajouter ..."



Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.

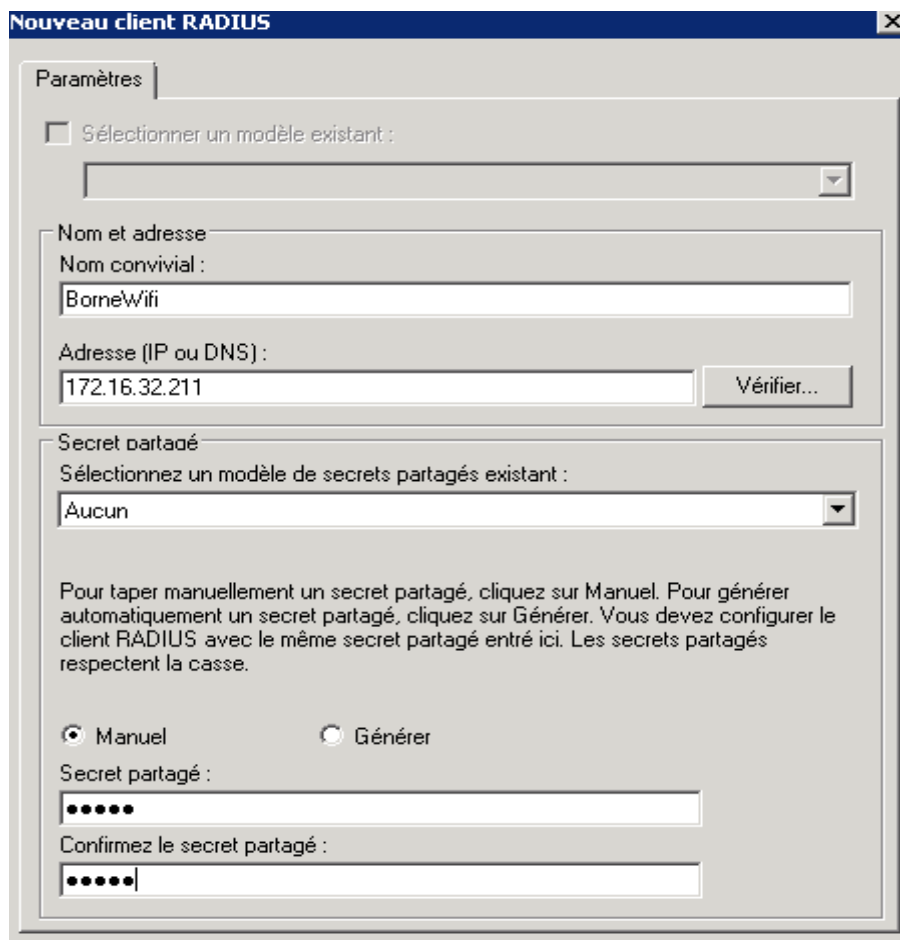
Pour spécifier un client RADIUS, cliquez sur Ajouter.

Clients RADIUS :

Empty list area for RADIUS clients

Ajouter...
Modifier...
Supprimer

Et saisissez vos paramètres et appuyez sur "OK".



Nouveau client RADIUS

Paramètres

Sélectionner un modèle existant :

Nom et adresse

Nom convivial : BorneWifi

Adresse (IP ou DNS) : 172.16.32.211

Secret partagé

Sélectionnez un modèle de secrets partagés existant : Aucun

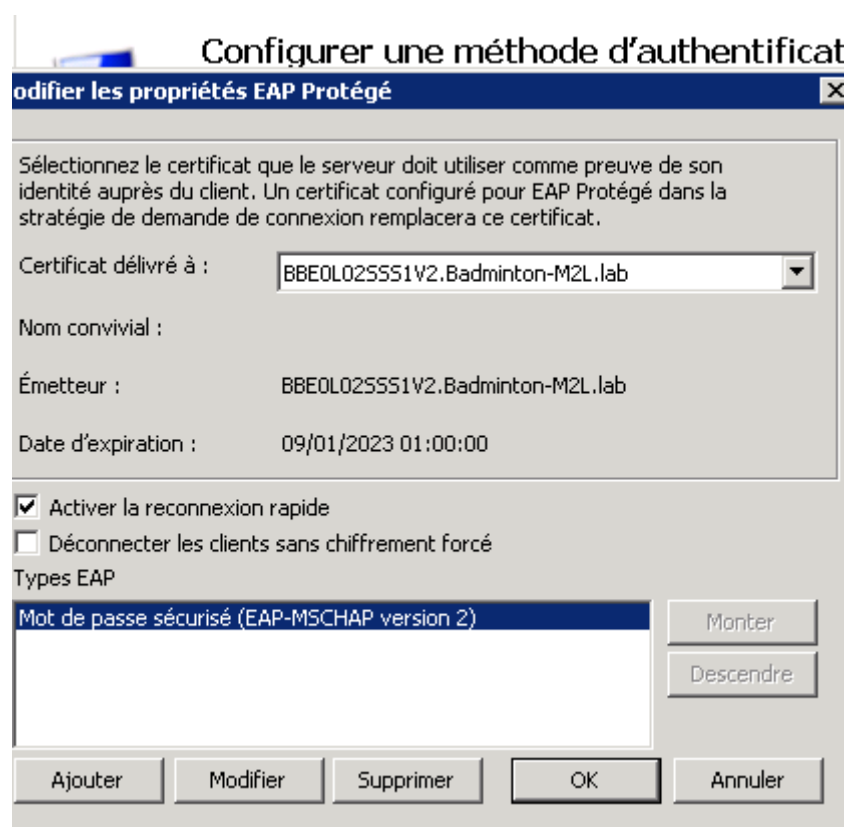
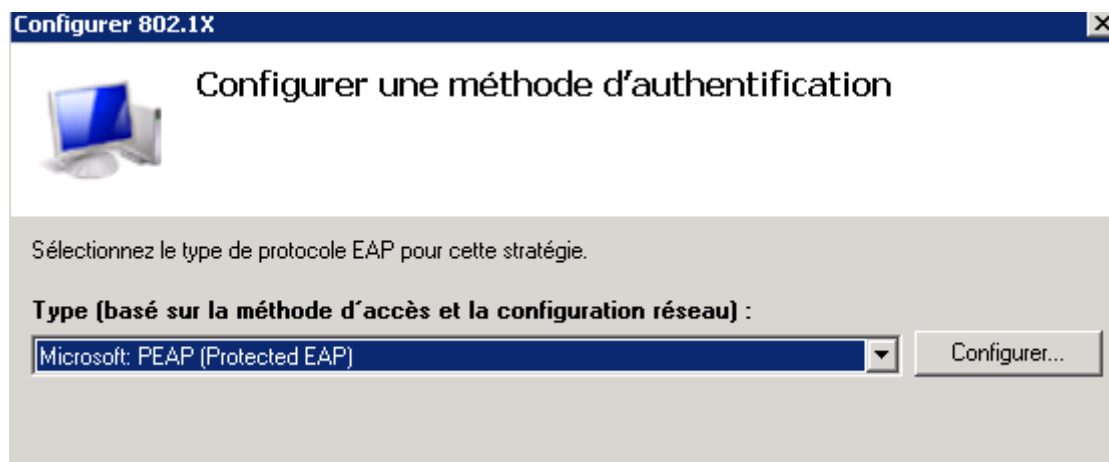
Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel Générer

Secret partagé :

Confirmez le secret partagé :

Voulez aller devoir choisir le type de protocole EAP faites dérouler le menu et sélectionner le "Microsoft PEAP (Protected EAP)" et cliquez "Configurer..." afin de modifier les propriétés EAP.



Une fois les modifications effectuées cliquez sur "Suivant".

Nous sommes arrivés à la fin de l'installation, vous venez d'installer un serveur Radius qui va permettre l'authentification.