

- Groupes et paramètres pour l'ensemble des TP (l'enseignant affectera les n° de groupe)

Groupe	Nom SSID	Réseau	@IP Switch	@IP AP	RADIUS	Clients
1	Angleterre	10.1.1.X/24	10.1.1.1	10.1.1.2	10.1.1.5	10.1.1.10 à 10.1.1.19
2	Belgique	10.1.2.X/24	10.1.2.1	10.1.2.2	10.1.2.5	10.1.2.10 à 10.1.2.19
3	Chypre	10.1.3.X/24	10.1.3.1	10.1.3.2	10.1.3.5	10.1.3.10 à 10.1.3.19
4	Danemark	10.1.4.X/24	10.1.4.1	10.1.4.2	10.1.4.5	10.1.4.10 à 10.1.4.19
5	Espagne	10.1.5.X/24	10.1.5.1	10.1.5.2	10.1.5.5	10.1.5.10 à 10.1.5.19
6	France	10.1.6.X/24	10.1.6.1	10.1.6.2	10.1.6.5	10.1.6.10 à 10.1.6.19
7	Grece	10.1.7.X/24	10.1.7.1	10.1.7.2	10.1.7.5	10.1.7.10 à 10.1.7.19
8	Hongrie	10.1.8.X/24	10.1.8.1	10.1.8.2	10.1.8.5	10.1.8.10 à 10.1.8.19
9	Italie	10.1.9.X/24	10.1.9.1	10.1.9.2	10.1.9.5	10.1.9.10 à 10.1.9.19
10	Luxembourg	10.1.10.X/24	10.1.10.1	10.1.10.2	10.1.10.5	10.1.10.10 à 10.1.10.19

NB 1 : Antenne « A » (= AC sur AP 3702i) = 5 Ghz, antenne « G » (= N sur AP 3702i) = 2,4 Ghz.

NB 2 : Ne JAMAIS utiliser les menus « express-setup » pour effectuer les exercices !

## 1. Installation et configuration d'une carte Wi-Fi/Dongle USB

- Installer le driver (*grand dongle noir* : AC1200, *petit dongle noir* : A6100, *dongle D-Link gris*=DWLAG132 : Vista 64bits) via le gestionnaire de périphérique de Windows.
- Pour Windows 2008R2, **installer la Fonctionnalité : Service de réseau local sans fil**.
- ✓ Avec l'utilitaire de recherche réseaux, rechercher et notez les réseaux disponibles.

## 2. Installation du logiciel NetStumbler/Vistumbler

- Lancer l'installation : utilisez le répertoire « Vistumbler\_v10-5-updated » pour 64 bits.
- Recherche des réseaux disponibles dans l'environnement.
- Voir les SSID, les canaux utilisés et les sécurisations sur ces différents réseaux ainsi que la cartographie (extra-> channel graph).
- ✓ Notez les réseaux que vous trouvez, comparez avec l'étape 1, puis **fermez Vistumbler**.

## 3. Installer un réseau Ad-Hoc (sans sécurité, xxx=votre pays)

- Utilisez « centre de réseau et partage », créez un réseau AD-HOC (AD\_xxx) sur un PC.
- Rejoignez ce réseau (« Gérer les réseaux sans fil », sélectionnez AD-HOC).
- ✓ Vérifier la connectivité par un ping (retirez le câble ethernet et désactivez le parefeu).
- Relancez Vistumbler, notez les nouveaux réseaux, puis fermez Vistumbler.
- Optionnel : Effectuez un partage de fichier.

## 4. Mise en place des AP (câblage et @IP selon groupes)

### • Installation physique et connexions des points d'accès Cisco

- Brancher physiquement les câbles, installer le convertisseur USB-série : le driver du convertisseur : « IUT Blackbox »), ainsi que le driver du port série (même répertoire).
- Effectuer une première configuration de l'AP via la liaison série avec TeraTerm :

```
(appuyez plusieurs fois sur <Entrer>)
AP> enable          (cf login à droite)
AP# configure terminal
AP(config)# Interface bvi1
AP(config-if)# ip address address mask
               → de l'AP
```

Login :	Cisco (sensible à la casse)
Password :	Cisco (sensible à la casse)

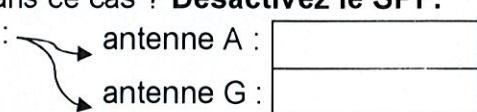
Uniquement en cas de besoin :

Reset AP en ligne de commande :	#write default-config #reload (Save : No)
---------------------------------	----------------------------------------------

### • Lors du premier accès à l'AP via un navigateur (et à chaque démarrage de TP)

- Dans gestionnaire de serveur Windows 2008, paramètres : retirer la sécurité renforcée.
- Retirer le bloqueur de popup (onglet confidentialité sur IE / options, contenu sur Firefox).
- Reset AP via HTTP : system software, system configuration, reset to default (except IP).

## 5. Installation d'un premier réseau WIFI en Infrastructure

- Créez un SSID avec le *nom de votre pays* sur les 2 antennes, activez le broadcast du SSID, vérifiez l'état des antennes, puis connectez les PC sur le réseau sans fil.
- Débranchez le câble ethernet ou désactivez l'interface Ethernet connectée à l'AP.
- Faites un ping entre les 2 machines connectées à l'AP, puis entre ces machines et l'AP.
- Activez le "Public Secure Packet Forwarding" (**SPF**) dans les interfaces radios.
- Faire un ping entre les 2 machines connectées à l'AP en Wifi, puis entre ces machines et l'AP, puis remettez un PC sur la partie filaire et faites un ping entre les 2 machines.
- ✓ A quoi sert cette option ? Quel est le rôle de l'AP dans ce cas ? **Désactivez le SPF**.
- Fixer les antennes de l'AP sur un canal bien précis :  antenne A :   
antenne G :
- ✓ Notez les valeurs du menu « Association » de l'AP.
- Lancer des pings en continu (-t) vers l'AP.
- Désactiver l'antenne radio **A/AC** puis réactivez-la avant de désactiver la **G/N**.
- ✓ Vérifiez la reprise de la connexion sur l'autre antenne et via le menu « Association ».

## 6. Analyse des trames 802.11 (dongle AC1200 pour la capture CA7)

- Installez Wirshark, (*lire installation.txt pour les consignes*), et capturez des trames.
  - Nota : débranchez le câble Ethernet ou désactivez l'interface Ethernet des 2 PCs.
- Installer le logiciel ComView (CA7) sur l'un des 2 PC disposant du dongle AC1200 afin d'effectuer des captures de trames, l'autre PC servant de générateur de trafic ; activez l'antenne G et désactivez l'antenne A ; sélectionnez le canal fixé (1-14) dans CA7.
- Utilisez dans CA7 l'onglet « packet », clic droit, filtre rapide pour sélectionner les trames.
- ✓ Retrouvez le paquet contenant le ping entre le PC n'ayant pas Comview et l'AP.
- ✓ Optionnel : analysez avec Comview une connexion http ou un telnet vers l'AP.

## 7. Mise en place de la sécurisation du réseau WiFi avec WEP

### EFFACER LA CONFIGURATION DE L'AP

- Sans mettre en place un broadcast du SSID sur l'AP (**IMPERATIF**), créez un SSID dont le nom est WEP\_xxx (xxx est le pays de votre groupe), rattachez-le à l'antenne **A**.
- Configurer la sécurité WEP, utilisez l'antenne « **A** », et le menu « WEP » + Mandatory.
- Effectuer la connexion manuelle des PC au SSID via le menu « gérer les réseaux sans fil » de Windows, et effectuer des pings entre ceux-ci.

## 8. Mise en place de la sécurisation du réseau WiFi avec WPA2-PSK

### SANS MODIFIER LA CONFIGURATION PRECEDENTE ! (et donc sans broadcaster de SSID)

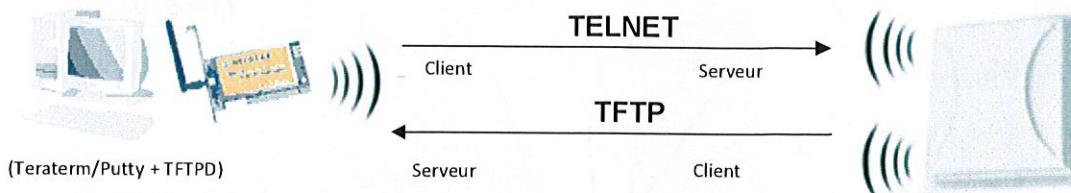
- Créez un autre SSID = WPA2-PSK\_xxx (xxx est le pays de votre groupe), à l'antenne **G**.
- Configurer la sécurité WPA2-PSK sur l'AP, utilisez l'antenne « **G** » et le menu « Cipher »
- Effectuer la connexion manuelle des PC au SSID, et effectuer des pings entre ceux-ci.
- ✓ Quels sont les contraintes pour faire plusieurs SSID ?
- ✓ Effectuez un ping entre 2 PC, l'un sur WEP l'autre sur WPA2. Le ping est-il ok ?
- ✓ Effectuez un ping des 2 PC, l'un sur WEP l'autre sur WPA2, vers l'AP. Le ping est-il ok ?
- ✓ Consultez les profils créés dans « gérer les réseaux sans fils » de Windows 2008R2.

## 9. Mise en place d'un serveur Syslog (optionnel)

- Dans l'« EventLog » de l'AP, « configuration options » configurez le renvoi des logs :
  - Syslog Server Host Name or IP Address : <IP du PC> (*choisissez la meilleure interface*)
- Lancez le logiciel **TFTPD32 ou TFTPD64**.
- Désactivez une antenne radio, puis tapez la commande « **reload** » sur l'AP.
- ✓ Vérifiez la bonne réception des événements dans l'onglet syslog du serveur TFTPD.
- ✓ Comparez la liste des événements dans « event log » sur l'AP et le syslog du TFTPD.

## 10. Sauvegarde et analyse du fichier de configuration

- Choisir un PC qui servira de serveur TFTP et lancer le logiciel *TFTPD32 ou TFTPD64*.
- Se connecter de ce PC en telnet (avec Teraterm ou putty) sur l'AP (via câble ou Wifi).



- Utilisez la commande : **copy running-config tftp:** (sur l'AP)
- Vérifiez qu'un fichier est créé sur le PC. L'ouvrir avec *notepad* puis *wordpad* et identifier :
- ✓ Quel est le nom de l'interface Ethernet ? des interfaces radios ? Pourquoi y en a-t-il plusieurs ? Sur quelle interface est positionnée l'adresse IP de management de l'AP ?

## 11. Mise en place d'un accès SSH (optionnel)

- Dans « Services », configurez Telnet/SSH, avec les paramètres ci-dessous :

<ul style="list-style-type: none"> <li>System Name: &lt;votre pays&gt;</li> <li>Domain Name: iut.paris13</li> <li>RSA Key Size: 1024</li> </ul>	<ul style="list-style-type: none"> <li>Authentication Timeout: 120</li> <li>Authentication Retries: 3</li> </ul>
-------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------

- ✓ Désactivez le telnet, et vérifiez le fonctionnement en SSH via TeraTerm.

- Optionnel : Activez le HTTPS (dans « services »).

*Nota : si besoin aller dans « Options Internet », « avancé », réactivez « SSL 3.0 » pour Internet Explorer.* ~~et les TLS~~

- ✓ Identifiez le certificat dans « security », « AP Authentication », onglet « Certificates » et comparez-le avec le certificat du navigateur.

Puis effacez la configuration de l'AP.

## 12. Configuration des VLANs

**Effacez la configuration de l'AP (reset AP) avant de démarrer cet exercice.**

- Créer des VLANs sur les AP, soit un VLAN **Guest** (VLAN n°2) et **Intranet** (VLAN N°3) à appliquer sur l'antenne adéquate (cochez « Native VLAN » pour le VLAN **Intranet**).
- Créez les 2 SSID ci-dessous et diffusez le SSID **GUEST\_xxx** uniquement.

Pensez à débranchez les câbles avant les tests.

SSID **GUEST\_xxx**  
VLAN 2 / Antenne A  
Sécurité WEP



SSID **INTRANET\_xxx**  
VLAN 3 / Antenne G  
Sécurité WPA2-PSK

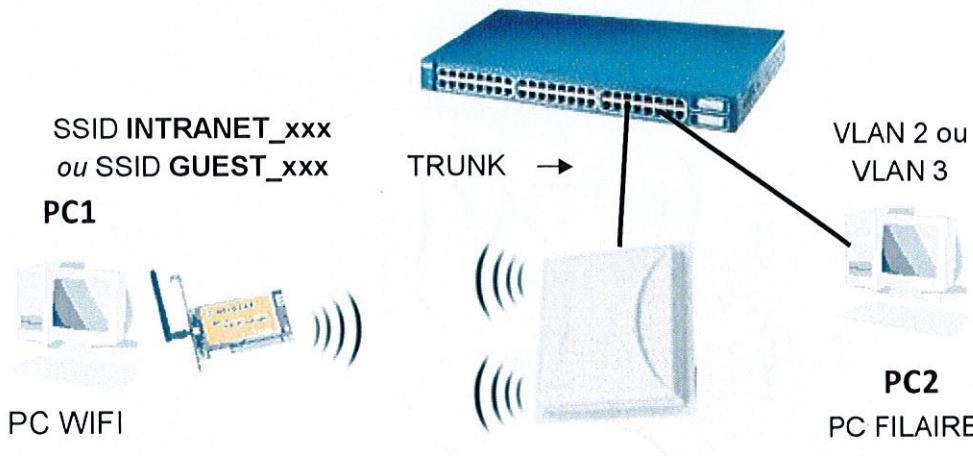


PCs	Test via ping	Résultat	
		VLAN 2	VLAN 3
VLAN 2	PC 1 vers PC 2		
	PC 1 vers AP		
	PC 2 vers AP		
VLAN 3	PC 1 vers PC 2		
	PC 1 vers AP		
	PC 2 vers AP		
PC1 Vlan3	PC2 Vlan2		

où xxx est le nom de votre pays.

- Connectez les PC sur l'un ou l'autre SSID correspondant à un VLAN et testez le tableau.
- ✓ Sur quoi est appliquée la sécurité (le cypher) / aux questions n°7-8 ?
- ✓ Les contraintes pour faire plusieurs SSID sont-elles différentes / questions n°7-8 ?
- ✓ Dans quel VLAN « est » virtuellement l'AP ? Pourquoi ?
- ✓ Faites « **show run** » ou récupérer la configuration dans « system software » : comment sont construites les interfaces radios et ethernet ? Comparez avec l'exercice n°10.

### 13. Configuration des VLANs entre AP et Switchs



Ping dans VLAN			Résultat	
PC 1	PC 2	AP		
2	2			
3	3			
3		AP		
	3	AP		

Après ajout de « native VLAN »			Résultat	
3	3			
2	2			
3	2			
3		AP		
2		AP		
	2	AP		
3	AP			

Cf tableau à droite

- Sur le commutateur, effacez les fichiers « **vlan.dat** » et « **config.text** » (commande « **del flash:vlan.dat** »), rebootez, créez les VLAN 2 et 3 et reliez l'AP via un lien « **trunk** » sur le port n°1, puis mettez le port 2 du switch dans le VLAN 2 et le port 3 dans le VLAN 3.
- Connectez le PC1 sur le SSID Guest (2) et le PC2 dans le VLAN 2 sur le switch.
- ✓ Testez le ping entre les 2 PC, l'un dans le VLAN 2 / l'autre sur le SSID Guest (2).
- ✓ Déplacez les connexions, l'un des PC dans le VLAN 3 et l'autre sur le SSID Intranet (3).
- ✓ Testez un ping de chaque PC vers l'AP.
- Modifiez le trunk sur le switch en ajoutant « **switchport trunk native vlan 3** ».
- ✓ ReTester le ping entre les 2 PC, l'un dans le VLAN 3 / l'autre sur le SSID Intranet (3).
- ✓ ReTester le ping entre les 2 PC, l'un dans le VLAN 2 / l'autre sur le SSID Guest (2).
- ✓ Vérifier l'étanchéité entre les 2 PC pour les PC dans un VLAN différent.
- ✓ Vérifiez l'accès à l'AP à partir du PC1 dans le SSID Intranet (3) puis le SSID Guest (2).
- ✓ Vérifiez l'accès à l'AP à partir du PC2 dans le VLAN 3 puis dans le VLAN 2.
- ✓ Quelle est la raison de ce comportement et à quoi sert la commande selon vous ?

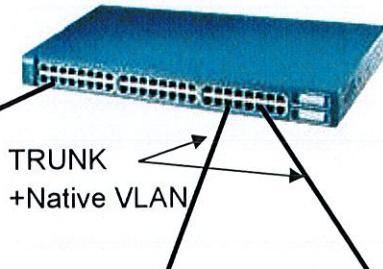
(A faire par groupe de 4 étudiants : faire le N°21 si attente d'un autre groupe)

- Construisez le réseau ci-après avec un autre groupe (soit 4 clients : 3 sans-fil, 1 filaire).  
Nota : GUEST\_xxx1 est le guest du 1<sup>er</sup> groupe et GUEST\_xxx2 le guest du 2<sup>ieme</sup> groupe.

#### GROUPE A

PC1 sur port dans VLAN 3

@IP =



PC3 SSID GUEST\_xxx1

@IP =



@IP =

#### GROUPE B

SSID INTRANET\_xxx2 PC2

@IP =



SSID GUEST\_xxx2 PC4

@IP =

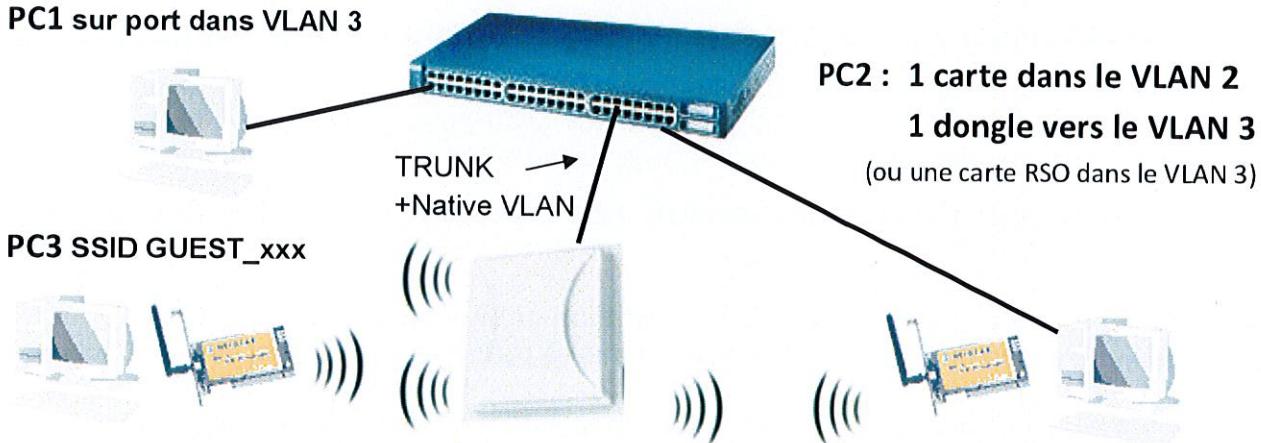


- Passez les masques des PC en /8, et pinger les PC.
- Activez le « Public Secure Packet Forwarding » sur les VLAN. Les PC 3 et 4 se voyent-ils ? Idem avec les PC 1 et 2.
- Tapez la commande « switchport protected » sur les interfaces du switch connectées aux AP. Les PC 1 et 2 communiquent-ils ? Idem pour les PC 3 et 4 ? Pourquoi ?
- Désactivez le « Public Secure Packet Forwarding ».

Ping entre PC				Résultat
PC 1	PC 2	PC 3	PC 4	
■	■	■	■	
■	■	■	■	
■	■	■	■	

- ✓ Optionnel 1 : Comment définir un réseau d'administration (non accessible par les utilisateurs) ?
- ✓ Optionnel 2 : Construisez le réseau ci-dessous, en attribuant un sous-réseau différent pour chaque VLAN 2 et 3, et en utilisant un rôle Windows pour le routage inter-VLAN.

PC1 sur port dans VLAN 3



- **PC2** : Avec le dongle WIFI, rattacher le PC2 au SSID Intranet et connecter le réseau filaire au VLAN 2. Si le PC possède 2 cartes (cas de la salle Q203), on peut utiliser la 2<sup>ième</sup> carte du PC pour mettre en place le routage, ou même router via 2 dongles WIFI. Installez et configurez le rôle « **service de stratégie et d'accès réseau** », avec 2 réseaux différents.
  - **PC1** : Positionnez-le dans le VLAN 3 sur un port du switch, et vérifiez la passerelle ;
  - **PC3** : Positionnez-le dans le SSID Guest (VLAN 2), et vérifiez la passerelle ;
  - ✓ Vérifiez la continuité de liaison entre PC1 et PC3.
- ✓ Optionnel 3 : Installer le « service DHCP » sur le PC2, créer les étendues et vérifier l'attribution d'une @IP au PC1 et PC3 quels que soit leurs positions dans les VLANs.

## 14. Création de comptes de sécurité sur l'AP (optionnel)

- Créez en Web, sur l'AP - menu « Admin Access » - un compte ADMIN\_R avec les droits de Read-Only et un compte ADMIN\_RW avec les droits Read-Write.
- ✓ Vérifiez si vous pouvez vous connecter.
- Sélectionnez « Local User List Only (Individual Passwords) »
- ✓ Vérifiez en vous connectant avec chacun des comptes si vous pouvez par exemple désactiver une antenne.
- Remettez l'authentification en « Default Authentication (Global Password) ».
- ✓ Vérifiez si vous pouvez vous connecter.
- Utilisez la console pour remettre un mot de passe : « **ena secret 0 Cisco** ».
- ✓ Vérifiez si vous pouvez vous connecter.
- ✓ En cas d'échec vous pouvez réinitialiser via : « **write default-config** » + « **reload** ».

## 15. Authentification et autorisation d'un AP via TACACS (optionnel)

- Installer l'application TACACS.net et notez le **shared secret**.
- Décochez l'attribut « lecture seule » pour les fichiers présents dans le répertoire caché « C:\ProgramData\TACACS.net\config\ ».
- Vérifiez que dans « clients.xml », il y a pour <ClientGroup Name="DEFAULT"> <Secret ClearText="le **shared secret**" DES=""></Secret>
- Modifiez « tacplus.xml » : <LocalIP>10.x.0.y</LocalIP> (@IP locale de Tacacs)
- Modifiez « authentication.xml » pour le groupe « Local System Administrators <LocalhostGroupName>**Administrateurs**</LocalhostGroupName>
- Autorisez sur le parefeu : « C:\Program Files (x86)\TACACS.net\tacplus.exe »
- Sur l'AP, dans « security » / « server manager », ajouter un serveur TACACS avec le **shared secret** et choisir ce serveur pour l'« Admin Authentication (TACACS+) ».
- Sur l'AP, dans « security » / « admin access », sélectionner « Authentication Server Only » et décocher « Enable Authentication Server Caching ».
- ⇒ Si besoin, redémarrez le service TACACS.net sur le serveur Windows 2008R2.
- ✓ Tentez une connexion WEB puis console avec le compte « Cisco » et « administrateur ».
- Ajoutez à authorization.xml pour « Local System Administrators », sous </UserGroups>
 

```
<AutoExec> <Set>priv-lvl=15</Set> </AutoExec>
      et sous <Shell> de ce même groupe (mais avant <Deny>.*</Deny>):
      <Permit>enable</Permit>
```
- Puis connectez vous via la console série afin d'ajouter ces lignes de configuration :
 

```
aaa authorization commands 15 default group tac_admin (Web)
      aaa authorization console (console)
```
- ✓ Déconnectez / reconnecter-vous sur la console/telnet et testez la commande « **conf t** ».
- Modifiez authorization.xml pour le groupe « Local System Administrators », sous <Shell>
 

```
<Permit>configure.*</Permit>
```
- ✓ Testez la commande « **conf t** » sur la console puis testez un accès en telnet, et WEB.
- ✓ Tentez la commande « **write default** » sur la console afin d'effacer la configuration.

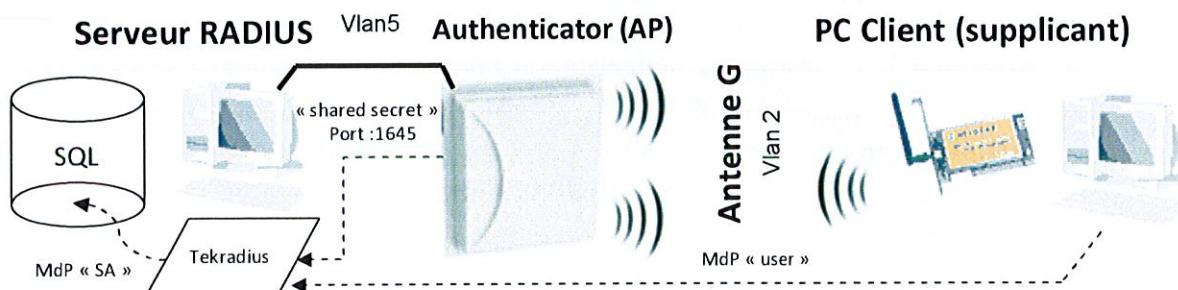
Puis effacez la configuration de l'AP via l'interface WEB.

## 16. Configuration du filtrage par adresses MAC (optionnel)

- Configurer le filtrage par adresses MAC sur les AP en utilisant les filtres d'adresses (créez un SSID = **WPA2-PSK\_xxx** si aucun SSID n'est existant).
- Connectez les PC sur le SSID afin de vérifier quelles sont les stations bloquées ou non.

## 17. Installation d'un serveur RADIUS avec WPA2 Entreprise

Attention : compter environ 2 heures minimum pour la réalisation de cet exercice : à faire dans l'ordre ci-dessous (il faut 15 à 20 minutes pour SQL Express).



- Pré-requis : Modifiez l'@ IP filaire du PC étant le serveur RADIUS (cf tableau page 1).
  - Dans la mesure du possible utilisez 3 mots de passe différents.

### a. Installation de l'AP (effacer toute configuration précédente)

- Créer le **VLAN 2** (sur l'antenne **A** et **G**) et le **native VLAN 5** (sur l'antenne **A**).
- Dans « Encryption Manager », pour le **VLAN 2**, choisir « Cipher = AES CCMP »
- Dans « Server Manager », créer un serveur Radius, et choisir un 'shared secret'
- Dans « SSID Manager », diffusez un SSID **WPA2-E\_xxx** avec :
  - Utilisation du **VLAN 2** et l'antenne **G**,
  - Choisir : Open Authentication : **with EAP + Network EAP: <NO ADDITION>**
  - EAP Authentication Servers, Customize et choisir le Serveur Radius créé,
  - Key Management : **Mandatory**, cocher **WPA**, mais ne pas mettre de clef.

### b. Installation du serveur RADIUS (autre choix : Microsoft NPS)

- Installer « dotNetFx40\_Client\_x86\_x64.exe »
- Installer SQL Express (si 32 bits : installer auparavant les 2 « MSInstaller-x86.exe »).
  - => Nouvelle Installation, puis accepter (case à cocher), et suivant 4x
  - Configuration du moteur : mode mixte ('sa'), choisir un mot de passe et suivant 2x
- Installer « tekCERT » (laisser les choix par défaut).
  - Lancer tekCERT, vérifiez l'heure du PC et que le choix est bien positionné à « Server Authentication », cliquer sur « Generate Certificate ».
  - Vérifiez via la MMC certificats qu'un certificat est bien présent sur le serveur (compte de l'ordinateur, personnel) puis exportez ce certificat via tekCERT (browse certificate) ou la MMC, sans la clef privée, sous le nom « **serveur.cer** »
- Installer « tekRadius » (laisser les choix par défaut)
  - Lancer tekRadius manager, et aller dans « settings »
  - Dans « SQL Connexion », mettre le mot de passe de 'sa', puis « save settings »
  - Dans « Database Tables », clic sur « create database » + « create Tables »
  - Dans « Service Parameters », mettre le port à 1645 (et Accounting à 1646)
  - Vérifier la valeur indiquée de l'adresse IP utilisée.
  - Revenir dans l'onglet client, choisir NAS=@IP de l'AP, mettre le « shared secret », cliquer sur « Add/update »
  - Démarrer le service (flèche verte dans « settings »),
  - Dans l'onglet « user », mettre un 'nom d'utilisateur', cliquer sur l'icône « + », puis dans « Attribute » de cet utilisateur, laisser « check », choisir « user-password », mettre un 'mot de passe utilisateur', puis cliquer sur l'icône à droite afin de valider la valeur. Enfin, ajouter l'attribut « TLS-Server-Certificate » = certificat du serveur.

### c. Installation du client

- Installer le certificat « **serveur.cer** » dans « Autorité de certification racine de confiance »
- Créer un profil Wifi manuellement avec le SSID, en WPA2-Entreprise, et pour sécurité :
  - PEAP => paramètres => sélectionner le certificat du serveur,
  - Dans MSCHAPv2, configurer, décocher « utiliser automatiquement mon nom... »
  - Décochez également « Mémoriser mes informations d'identification ».
- ✓ Tester la connexion, avec 'nom d'utilisateur' et 'mot de passe utilisateur', puis vérifiez l'accès (ping) à un autre équipement (smartphone) que vous connecterez à ce SSID de l'AP et/ou vérifiez le VLAN affecté à l'équipement dans le menu « Association » de l'AP.
- Optionnel - **VLAN Dynamique** : créer le **VLAN 3** (sur l'antenne **G**) avec « Cipher = AES CCMP », puis dans TekRadius, sélectionner dans Groups le groupe « **Default** » avec :
  - Success-Reply : - Tunnel-Medium-Type= « 802 »
  - - Tunnel-Type= « VLAN »
  - - Tunnel-Private-Group-ID = « 3 » (ensuite « 2 ») (n° VLAN)
- ✓ Connectez-vous et vérifiez le VLAN affecté via le menu « Association » de l'AP pour chacun des numéros de VLAN, puis supprimez ces 3 lignes du « Groups Default ».

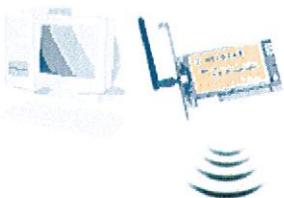
## 18. Mise en place d'un pont Wifi (optionnel) avec des AP 3702i

(Exercice à faire par groupe de 4 étudiants : attendez n'importe quel autre groupe)

- Effacer les configurations de l'AP non Root et mettre en place le réseau ci-dessous :

**GROUPE A (AP Root)**

N° de groupe =X, pays=xxx



@IP =

**GROUPE B (AP non-Root)**

N° de groupe =Y, pays=yyy

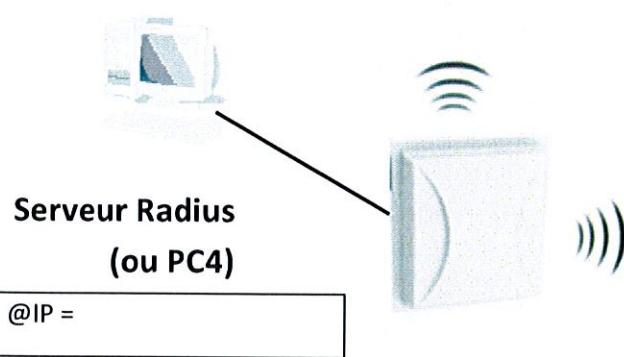


@IP =

PC2

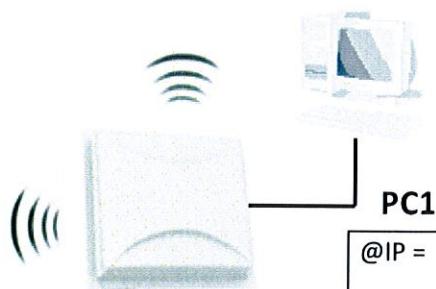
SSID WPA2-E\_xxx / SSID WPA2-PSK\_xxx  
Antenne G / Vlan 2

SSID WPA2 \_yyy  
Antenne G / Vlan 2



@IP =

SSID BR\_X\_Y (INFRASTRUCTURE)  
Antenne A / Native Vlan 5 (+ vlan 2)



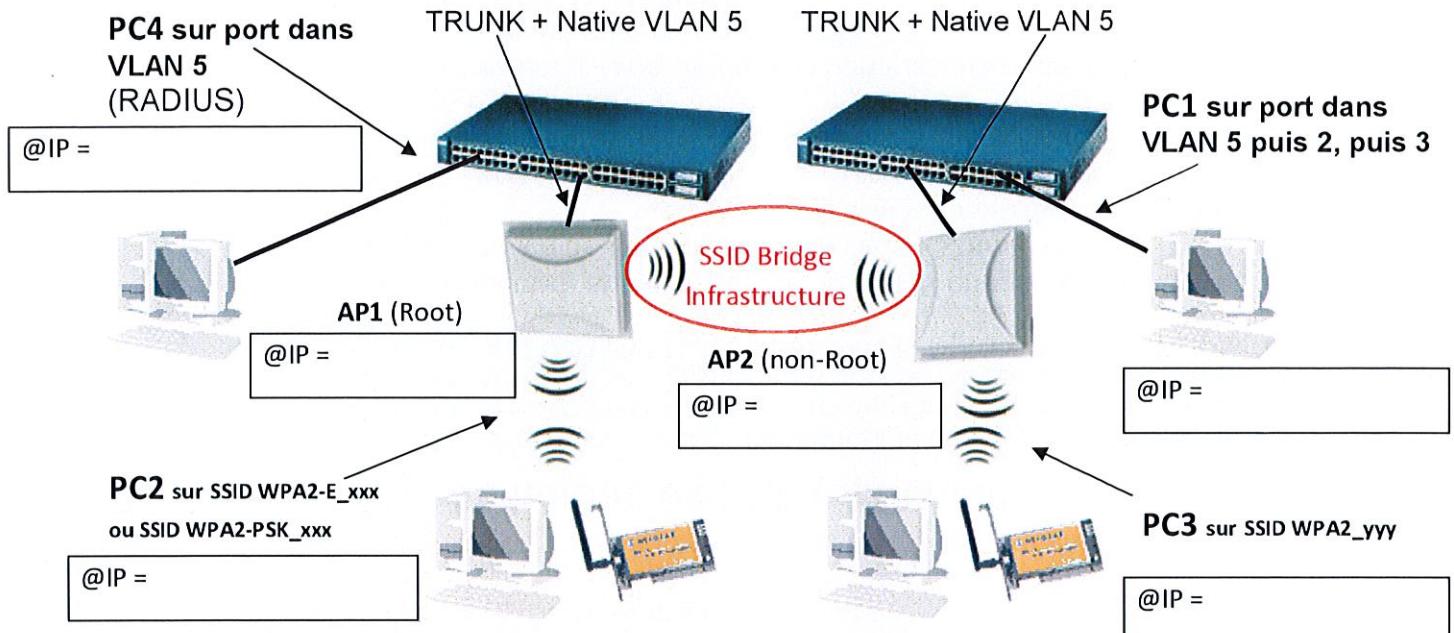
@IP =

PC3

- Modifiez les masques des PC et des AP en /8.
- Sur l'AP Root, dans l'interface de l'antenne **A** utilisée pour l'interconnexion, passer l'interface de l'AP en **Root bridge**, et créer un SSID **BR\_X\_Y, VLAN 5** (native), **antenne A**, puis le sélectionner en tant que SSID d'Infrastructure en cochant « force infrastructure »). Ne pas le diffuser. NB : au besoin créer un SSID **WPA2-PSK\_xxx** sur l'antenne **G** et le **VLAN 2** si l'exercice précédent sur RADIUS n'a pas été fait sur l'AP.
- Sur l'AP non Root, créez les **VLAN 2** (antenne **G**) et **VLAN 5 : native** (antenne **A**), puis créer le SSID **BR\_X\_Y** avec le **VLAN 5** et l'antenne **A**, sélectionner ce SSID en tant qu'Infrastructure en cochant « force infrastructure ». Enfin dans l'interface de l'antenne **A** utilisée pour l'interconnexion passer l'AP en **Non Root bridge**. Ne pas le diffuser.
- ✓ Vérifiez le menu « Association » des 2 AP. Notez les différences avec l'exercice n°5.
- ✓ Vérifiez qu'un PC client ne peut pas se connecter au SSID **BR\_X\_Y**.
- ✓ Vérifiez le bon fonctionnement du ping entre le serveur Radius (ou PC4) et PC1.
- Mettre en place un SSID **WPA2\_yyy** sur l'antenne **G** de l'AP non Root, protégé en **WPA2-PSK** sur le **VLAN 2**, que vous diffuserez.
- ✓ Vérifiez le non-fonctionnement du ping entre PC2 et PC3. Ajoutez le **VLAN 2** sur l'antenne **A** (sur les 2 AP), puis revérifiez. Notez qu'il n'y a pas de « trunk » déclaré !
- Optionnel 1 : mettez une sécurité **WPA2-PSK** sur les AP Root et non Root pour le SSID **BR\_X\_Y** (c'est-à-dire sur le **VLAN 5**).
- ✓ Vérifiez le bon fonctionnement du ping entre PC2 et PC3 et entre PC1 et le serveur Radius (PC4), et l'échec des pings entre PC2 et PC1 ainsi que PC2/PC4, PC1/PC3.
- Optionnel 2 : configurez l'AP du groupe B de manière à utiliser le serveur RADIUS du groupe A pour le SSID **WPA2\_yyy**. Testez avec le PC3.

## 19. Switchs, VLAN et pont WIFI (optionnel, suite de l'exercice n°18)

- Insérer des switchs afin de mettre en place le réseau ci-dessous :



- Vérifiez le ping entre les PC selon leur positionnement dans les VLANs.

PC1 dans	AP1	AP2	PC2	PC3	PC4
VLAN 5					
VLAN 2					
VLAN 3					

## 20. Supervision d'un AP Cisco via SNMP (optionnel)

- Dans « Services », configurez SNMP avec les paramètres ci-dessous :
  - Simple Network Management Protocol (SNMP) : **enable**
  - System Location (optional) : **Q203** (ou P202 / la salle de TP)
  - System Contact (optional) : <**votre ou l'un de vos noms**> (APPLIQUEZ)
  - Dans « **SNMP Request Communities** », sélectionnez « **Public** » et effacez la valeur présente dans le champ « **Object Identifier (optional)** » (APPLIQUEZ)
  - Dans « **SNMP Trap Community** », indiquez dans « **SNMP Trap Destination** » l'adresse IP de la carte filaire de votre PC, puis cochez « **Enable All Trap Notifications** » (APPLIQUEZ)
- Installer et lancez le logiciel « **setup-mib-browser.exe** », puis configurez-le :
  - Déchargez toutes les MIBs (menu *File, UnLoad MIBs*).
  - Chargez les 10 premières MIBs du répertoire « **MibsAPCCisco** » (dans les fichiers copiés à partir du serveur - cliquez sur la première, puis avec shift sur la dernière) – soit toutes les MIBs sauf « **5.ENTITY-MIB-V1SMI.my** ».
- Connectez un PC sur l'AP via une connexion filaire et avec l'autre PC en Wifi.
- Accédez à l'AP avec le MIB Browser (comme avec un site Web).
- La branche **mib2** est la MIB « de base », répondant à la RFC1213 :
  - Recherchez et notez : le nom de votre système, la localisation, et le contact.
  - Modifiez **System Name** dans **Services-Telnet/SSH** de l'AP (Web), revérifiez la valeur.
  - Depuis combien de temps le système est démarré ?
  - Identifiez les interfaces, combien y en a-t-il ?

- La branche **private** regroupe les valeurs propres au constructeur :
  - ✓ Recherchez la table permettant d'avoir des informations sur les clients connectés.
  - ✓ Recherchez la table contenant les SSID existants.
  - ✓ Recherchez la table contenant les VLANs existants.
  - ✓ Recherchez la table contenant la méthode de chiffrement actuelle sur les VLANs.
  - ✓ Recherchez la table contenant la liste des clients connectés à l'AP et notez leurs @IP
- Sur l'AP (en Web), dans « **EventLog** », « **configuration options** », cochez **Record for SNMP/Syslog History Table** pour « **Notification** » et « **Information** », puis mettez **100** dans la valeur « **History Table Size** ».
  - ✓ Recherchez la table contenant les logs de l'AP.
- Démarrez l'enregistreur de TRAP (*trap receiver*), puis redémarrez l'AP (option *restart*).
  - ✓ Identifiez le trap correspondant à la commande de redémarrage.
  - ✓ Quels sont les autres traps ?
- Déchargez la MIB « **3b.CISCO-DOT11-IF-MIB-V1SMI.my** » et chargez la MIB « **5.ENTITY-MIB-V1SMI.my** ». Cliquez sur le trap ayant uniquement des chiffres.
  - ✓ Quelle est sa signification ?
  - ✓ Pour voir l'apport de chaque MIB, dans *Tools-Options*, décochez *Single Tree Root*.
- Sur l'AP, cocher **Debugging** dans les options du menu **EVENT LOG** pour **Record for SNMP /Syslog History Table** ainsi que **Notify via SNMP /Syslog Trap**.
  - ✓ Tenter une connexion d'un PC sur un SSID avec un mauvais mot de passe pour regarder le résultat dans les logs de l'AP et dans les TRAPs du MIB Browser.

## 21. Mise en place d'un DHCP sur l'AP (optionnel)

- Dans la console de l'AP, activez un serveur DHCP avec les paramètres ci-dessous :

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 10.1.X.1 10.1.X.20
AP(config)# ip dhcp pool plage_wifi_DHCP
AP(dhcp-config)# network 10.1.X.0 255.255.255.0
AP(dhcp-config)# lease 10 [ou infinite] (nombre de jour de bail)
AP(dhcp-config)# default-router 10.1.X.254
AP(dhcp-config)# end
```

- ✓ Testez l'attribution d'une adresse IP à votre PC sur le *native VLAN*.

## 22. Synchronisation horaire de l'AP (optionnel)

- Sur votre serveur Windows 2008R2, configurez le serveur NTP via REGEDIT :
  - **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type=NTP**
  - **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags=5**
  - **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer\Enabled=1**
- Sur le parefeu Windows, autorisez le port 123/UDP entrant (ou désactivez le parefeu).
- Enfin, lancez le service de temps par : **net start w32time**  
 (ou dans la console des services « Temps Windows »)
- Sur la partie WEB de l'AP :
  - Activez le service **SNTP - Simple Network Time Protocol** et choisissez l'@IP de votre serveur Windows ;
  - Sélectionnez dans *Time Settings* le bon fuseau horaire (GMT Offset) ;
  - Ne mettez pas d'heure manuellement ;
  - Validez la saisie des paramètres.
- ✓ Au bout de quelques secondes, vérifiez la mise à jour du temps dans la page WEB du service SNTP.
- ✓ Effectuez une action simple (exemple : désactivation d'une antenne) puis allez voir l'heure et l'action associée dans les logs de l'AP (Event Log).