

Laboratoire de téléinformatique, TIN

Réseaux sans fil : Couche physique, analyseur et sécurité

Si vous êtes déjà familiarisé-e avec l'une ou l'autre des manipulations dans ce laboratoire, vous pourrez les réaliser plus rapidement que le reste de la classe. Dans l'intérêt du groupe, veuillez laisser s'il vous plaît le temps aux autres de comprendre les manipulations et faites-leur profiter de vos connaissances en leur expliquant s'ils ou elles en ont besoin.

N'utilisez **pas** les réglages de sécurité pour les expériences de ce travail pratique.

Matériel

Stations

Deux types de stations de travail sont mises à disposition sur chaque poste de travail. La station à gauche possède un dispositif de capture et d'analyse de trames (AirPcap) avec la nouvelle version d'Ethereal dont le nom est Wireshark, capable de décoder les trames wifi. La station au milieu possède une interface sans-fil standard. Sur ces stations vous disposez d'un outil permettant la détection de tous les réseaux y compris ses SSID et canaux respectifs (Network Stumbler). Un répertoire partagé (Fichiers) se trouve sur le desktop de chacune de ces stations. Les stations de droite ne seront pas employées.

Access Points

Six points d'accès/routeurs (AP) Linksys WRT54GS sont à disposition

Autres

Câbles Ethernet, hubs, switches

Etablissement d'un réseau ad-hoc

Organisez vous en groupes de deux. Mettez vous d'accord entre groupes pour établir deux réseaux sans-fil indépendants en configuration ad-hoc.

Faites-le sous Windows avec la Zero Configuration

Quels sont les réglages dont vous avez eu besoin ?

Pensez à deux applications dans lesquelles il serait utile et intéressant d'utiliser de réseaux ad-hoc ?

Quand vous aurez fini cette partie, un enseignant ou une enseignante vous montrera comment partager une présentation PowerPoint à travers un réseau ad-hoc si, para exemple, vous ne disposez pas de beamer.

Les réseaux infrastructure

Les réseaux infrastructure nécessitent l'utilisation d'un point d'accès. Formez deux groupes et établissez deux réseaux infrastructure indépendants avec les AP fournis. Justifiez brièvement ci-dessous vos choix des paramètres.

Dans les répertoires partagés « Fichiers » qui se trouvent sur le bureau de chaque station du milieu, vous trouverez 3 fichiers identifiés comme 50M, 100M et 200M mesurant 50, 100 et 200 mégaoctets respectivement. Pour avoir une idée des performances de votre réseau, transférez un ou plusieurs de ces fichiers afin de mesurer le débit de la transmission.

Notez votre résultat ici : _____ bps

Formez des groupes de deux personnes et essayez avec votre partenaire pour répondre à la question suivante : si vous devez ajouter un quatrième réseau dans la salle, quelle stratégie utiliseriez-vous pour la sélection des canaux (on suppose que vous pouvez changer les réglages de tous les points d'accès) ? Vous avez dix minutes pour préparer votre proposition. Chaque groupe pourra présenter sa solution aux autres pour discussion.

Afin d'étudier l'effet du choix du canal, vous allez faire quelques mesures. Vous allez former des groupes encore une fois. Les indications pour leur formation seront données par les enseignant-e-s.

Les tests à effectuer sont les suivants : faites deux transferts de fichiers en parallèle en utilisant deux réseaux basés sur infrastructure que vous réglerez pour qu'ils utilisent le même canal. Mesurez le débit de transfert en utilisant la technique suivante : démarrez sur un réseau le transfert du fichier le plus grand (200 Mo). Pendant cette transmission, transférez le fichier le plus petit (50 Mo) sur l'autre réseau et mesurez le débit de cette dernière transmission. Demandez aux enseignant-e-s quels canaux utiliser.

Notez votre résultat ici : _____ bps (même canal)

Répétez l'expérience en utilisant deux réseaux espacés d'un canal et ensuite de deux canaux.

Notez votre résultat ici : _____ bps (un canal de séparation)

_____ bps (deux canaux de séparation)

En vue de ces résultats, quelle stratégie proposeriez-vous pour le réglage de fréquences de quatre points d'accès installés dans le même local ?

Analyse de trafic

Démarrez Wireshark et capturez des trames provenant des réseaux sans-fil visibles dans la salle (s'il n'y en a pas, vous pouvez le créer).

1. Quelle est la trame la plus fréquente ?

Souvenez-vous qu'il y a trois types de trames MAC utilisées dans les réseaux 802.11X : trames de données, trames de contrôle et trames de management.

2. Quelles trames de contrôle observez-vous dans vos captures ?

3. Quelles trames de management observez-vous dans vos captures ?

4. Dessinez un diagramme en flèche correspondant à une transmission de données CSMA/CA. Cherchez de tels échanges dans les séquences de trames capturées. Essayez de trouver la valeur de SIFS : _____

5. Afin d'observer des échanges de trames en RTS/CTS, changez le seuil RTS d'un des points d'accès.
6. Faites une capture et représentez à l'aide d'un diagramme en flèche vos observations pour une transmission entre deux stations associées au même point d'accès.

7. Afin de vous familiarisez avec quelques champs dans les trames, notez la valeur du champ « duration » pour quelques trames (RTS, CTS, ACK, Données). Quelle est la signification de ce paramètre ?

8. Observez aussi les champs ToDS et FromDS. Quelle est la valeur de ces deux dans les trames de contrôle ?

9. Voyez-vous dans vos captures l'évidence du mode de protection ? Expliquez l'évidence et ce que c'est. S'il n'y en a pas, essayer de forcer le mode protection.

10. Faites une capture pendant le démarrage d'un réseau et donnez la séquence de trames dans un diagramme en flèche.

11. Quel type d'authentification avez-vous observée ?

Sécurité

Etablissez un réseau sécurisé WEP (utilisez l'annexe sécurité).

1. Faites une capture pendant les phases initiales d'association à un réseau et donnez la séquence de trames dans un diagramme en flèche.

2. Répétez l'expérience avec un réseau sécurisé en WPA Personal

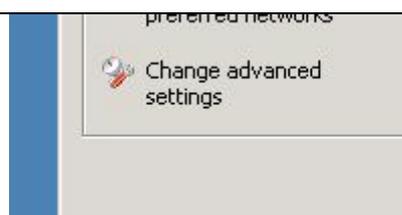
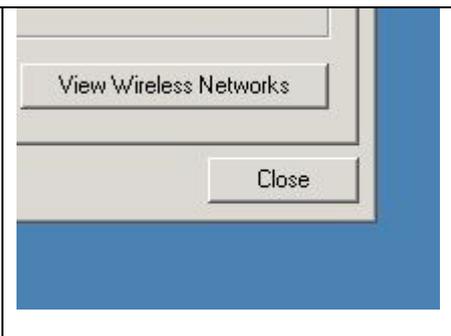
3. Dans la salle où vous vous trouvez, on a établi un réseau qui présente certaines failles de sécurité et d'optimisation. On vous demande d'étudier le problème, d'identifier les fautes et de proposer des solutions et des optimisations. Vous avez accès aux AP (adresses IP 192.168.1.1 et 192.168.1.2) et aux stations.

Annexe 1 : Etablissement d'un réseau ad-hoc

Si vous n'avez pas encore établi de connexion sans fil, cliquez sur l'icône de l'interface sans fil

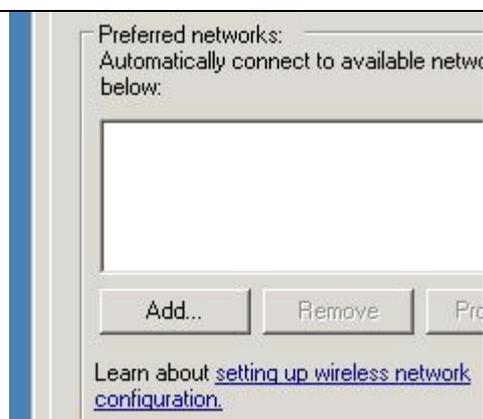
non-connectée  pour ouvrir la fenêtre de sélection de réseaux sans fil disponibles.

Si vous vous trouvez déjà connecté à un réseau, vous aurez la fenêtre d'état de la connexion en cours. Pour passer à la fenêtre de sélection de réseaux, il suffit de cliquer sur « View Wireless Networks ». La fenêtre de sélection de réseaux vous présente les différents réseaux sans fils se trouvant à portée de votre interface.



Nous allons procéder à définir les paramètres du réseau ad-hoc, qui sera ensuite disponible sur la liste de sélection de réseaux pour que d'autres utilisateurs puissent y accéder. Cliquez donc sur « Change advanced settings »

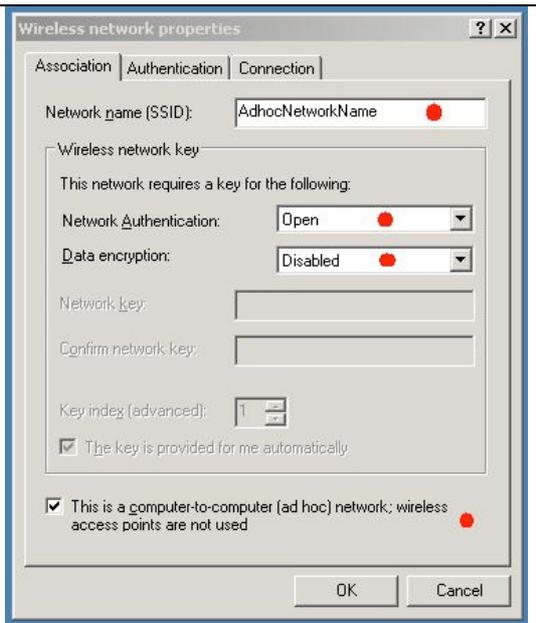
Sur la nouvelle fenêtre « Wireless Network Connection Properties » qui s'ouvre, choisissez l'onglet « Wireless Networks »



Vous avez maintenant la possibilité de modifier les paramètres des réseaux sans-fil déjà configurés ou d'en ajouter des nouveaux. En effet, une liste des réseaux préférés (réseaux sans-fil auxquels vous vous êtes déjà connecté dans le passé) s'affiche. Vous pouvez choisir d'éliminer un réseau (Remove), d'en modifier un (Properties) ou d'en ajouter un (Add). Cliquez donc sur « Add... »

La fenêtre de « Wireless network properties » vous donne la possibilité de choisir ou définir les caractéristiques du réseau sans-fil auquel vous voulez appartenir. Dans le cas d'un réseau ad-hoc dont vous êtes le créateur ou la créatrice, ces paramètres sont à définir. Si vous êtes en train de régler l'accès à un réseau existant, les paramètres doivent être choisis en fonction de valeurs données par la ou le responsable du réseau.

Dans notre cas, le réseau ad-hoc, ajoutez un SSID défini par vous-même et cochez l'option « This is a



computer-to-computer (ad hoc) network; wireless access points are not used », ce qui identifie le réseau comme un réseau ad-hoc. Dans cette expérience, nous allons laisser la sécurité de côté.

Le service APIPA (Automatic Private IP Addressing) de Windows se chargera d'attribuer des adresses IP à chaque station participant au réseau. Ces adresses sont choisies de manière aléatoire par le service. Pour s'assurer d'éviter les conflits d'IP, une requête ARP s'effectue avant d'attribuer finalement l'adresse choisie. La sélection manuelle d'adresses IP peut être plus intéressante en fonction des besoins et du scénario.

Annexe 2 : Etablissement d'un réseau infrastructure

Soit en utilisant le système de « Zero Configuration » pour les réseaux sans-fil de Windows, soit en utilisant les interfaces propriétaires des drivers des cartes réseau pour le paramétrage, la plupart de réglages d'un réseau basé sur infrastructure doivent être configurés au niveau du point d'accès.

Chaque fournisseur propose des points d'accès différents, vous permettant parfois d'agir sur des paramètres avancés du réseau sans-fil afin d'améliorer la sécurité ou les performances. Certains points d'accès incorporent un routeur et/ou un modem, ce qui permet le partage sans-fil d'une connexion Internet. Toutefois, il y a un certain nombre de paramètres qui « déterminent » en réalité le réseau. Ces paramètres se trouvent sans exception sur tous les modèles de points d'accès de toutes les marques.

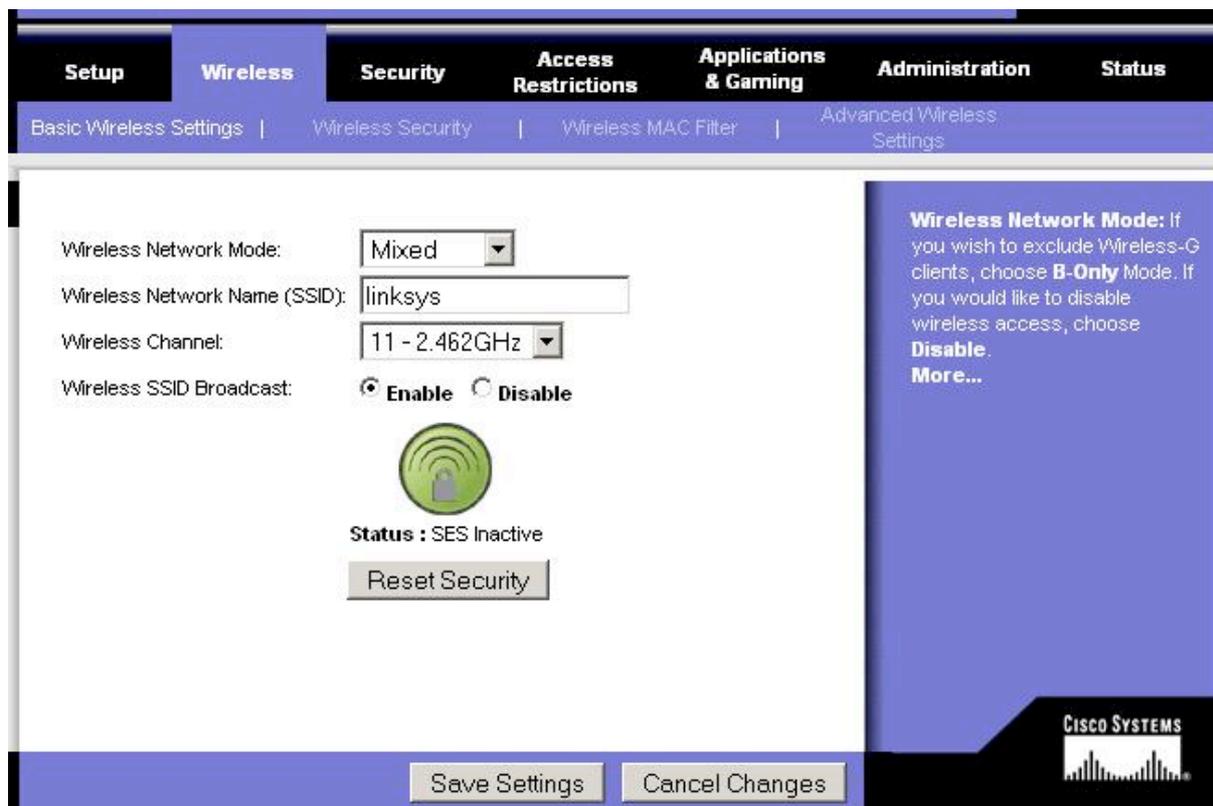
Notre travail de laboratoire utilise le point d'accès/routeur Linksys WRT54GS. Ce point d'accès propose une interface web pour faciliter l'introduction de paramètres de réglage. L'adresse IP par défaut du point d'accès est 192.168.1.1. Pointez votre navigateur internet vers cette adresse. Vous êtes invité-e à introduire le nom d'utilisateur ou utilisatrice et le mot de passe. Ils sont tous les deux « admin », les valeurs par défaut du point d'accès.



Un menu dans la partie supérieure de l'écran vous permet de naviguer dans les différentes options du point d'accès. La page principale appelée « Setup » vous permet de configurer un

serveur DHCP qui distribue des adresses IP aux stations faisant partie du réseau infrastructure. Cliquez sur l'onglet « Wireless » pour accéder à l'interface de configuration des réglages sans-fil

Les réglages de base « Basic Wireless Settings » s'affichent par défaut. Un sous-menu vous présente des onglets supplémentaires qui vous permettent de régler, entre autre, des paramètres de sécurité et certains paramètres avancés.



Une fois les réglages introduits et enregistrés (avec le bouton « Save Settings »), les stations peuvent rejoindre le réseau infrastructure. L'utilisation de la « Zero Configuration » de Windows facilite la tâche vous informant normalement que des réseaux sans-fil ont été détectés.

Cliquez sur le message ou sur l'icône de l'interface sans-fil pour accéder à la fenêtre de sélection de réseaux.



La liste de réseaux sans-fil à portée de votre interface s'affiche. Double-cliquez sur le réseau désiré pour vous y associer.

Annexe 3 : Etablissement d'un réseau sécurisé

Lorsque l'on sécurise un réseau sans-fil, il faut s'assurer que toutes les stations sont compatibles avec les méthodes de cryptage et protection sélectionnées, étant donné que certaines de ces méthodes sont récentes et ne sont pas universellement supportées.

La protection dans un réseau est imposée par le point d'accès. C'est à cet endroit où elle est définie en premier lieu.

Protection WEP

Point d'accès WRT54GS

Accédez au point d'accès comme vous l'avez fait dans le travail pratique de la semaine dernière (rapportez-vous à l'annexe « Etablissement d'un réseau infrastructure »). Suivez le lien « Wireless » qui vous amène aux paramètres du réseau sans-fil et ensuite, cliquez sur l'onglet « Wireless Security ». Dans la liste « Security Mode », vous pouvez sélectionner les différentes méthodes de sécurité que vous avez étudiées dans la théorie (à ne pas confondre avec l'onglet « Security » tout court). Cliquez sur WEP.



L'interface de paramétrage WEP vous permet alors de sélectionner un cryptage 64 bits ou 128 bits. Notez que la clé de 64 bits est en réalité une clé de 40 bits à laquelle on ajoute les 24 bits du vecteur d'initialisation IV qui sont transmis en clair. Également, pour la clé de 128 bits, il s'agit réellement d'une clé secrète à 104 bits plus les 24 bits du IV. Les clés utilisées avec WEP doivent être composées de combinaisons de caractères

hexadécimales. Le cryptage à 64 bits requiert 10 caractères hexadécimaux et celui à 128 bits, 26 caractères hexadécimaux. Pour faciliter la tâche de sélectionner des clés relativement faciles à déployer par les utilisateurs et utilisatrices du réseau, certains points d'accès vous permettent d'utiliser un mot ou une phrase qui sera ensuite utilisée par le point d'accès pour générer les séquences hexadécimales. Cette solution étant dépendante du fabricant, elle n'est pas toujours applicable, surtout lorsque l'on mélange des marques différentes d'interfaces sans-fil. La Windows Zero Configuration est toutefois capable d'interpréter dans beaucoup de cas les

mots ou phrases et de générer la séquence de caractères correspondante, mais avec une restriction : le mot générateur doit contenir exactement 5 caractères pour le cryptage 64 bits et 13 pour le cryptage 128 bits.

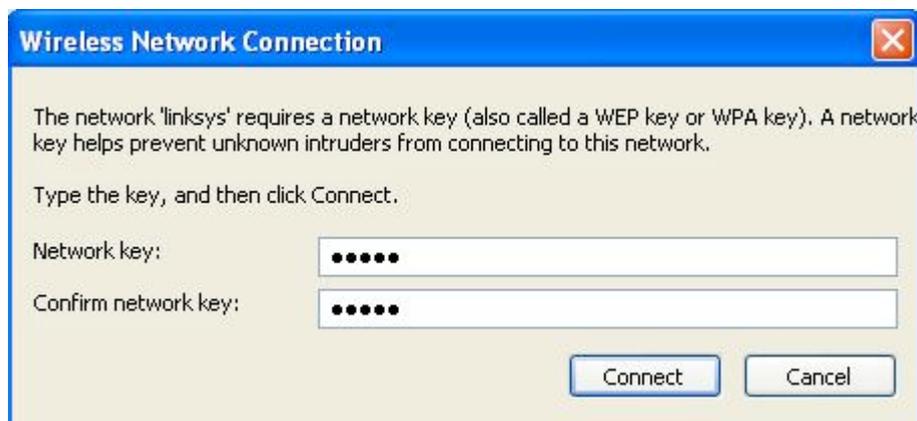
Security Mode:	<input type="text" value="WEP"/>
Default Transmit Key:	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
WEP Encryption:	<input type="text" value="64 bits 10 hex digits"/>
Passphrase:	<input type="text" value="unmot"/> <input type="button" value="Generate"/>
Key 1:	<input type="text" value="19AC1B849A"/>
Key 2:	<input type="text" value="1A43FE9912"/>
Key 3:	<input type="text" value="BCAF6E1E38"/>
Key 4:	<input type="text" value="96EA58BCB2"/>

Windows Zero Configuration

Quand vous essayez d'accéder au réseau sécurisé depuis votre station Windows, un cadenas et l'information « Security-enabled wireless network » vous annoncent que le réseau est protégé par un système d'cryptage.



Essayez de vous connecter au réseau sécurisé. Windows vous demande d'introduire la clé du réseau (deux fois pour confirmer que vous ne vous trompez pas en tapant).



Le mot que vous donnez pour vous connecter au réseau protégé WEP peut être le mot générateur de la clé que vous avez utilisé sur le point d'accès ou la propre clé à 10 ou 26 caractères hexadécimaux. Attention : si Windows ne parvient pas à générer la bonne séquence hexadécimale à partir du mot clé, il ne vous indique pas du tout qu'il n'a pas réussi. Dans ce cas là, vous ne recevrez pas d'adresse IP valable et vous ne serez évidemment pas connecté-e au réseau sécurisé. Il est donc conseillé d'utiliser la séquence hexadécimale. A partir du moment où vous vous identifiez avec la bonne clé WEP, vous êtes accepté-e dans le réseau et vous pouvez utiliser tous ses ressources.

Protection WPA

Point d'accès WRT54GS

Allez jusqu'à l'onglet « Wireless Security » comme vous l'avez fait pour la configuration de la protection WEP. Sélectionnez cette fois-ci la protection WPA Personal ou WPA2 Personal (ce dernier est seulement supporté par les modèles d'interfaces de cartes sans fil les plus récentes). En fonction du mode de sécurité sélectionné (WPA ou WPA2), des algorithmes de cryptage différents peuvent être choisis (TKIP, AES, TKIP+AES). La protection utilise également une clé, mais puisque dans le cas de WPA la clé est composée de 64 caractères hexadécimaux, elle est introduite sous la forme d'une phrase clé appelée « *pass phrase* ». Ce mot doit contenir un minimum de 8 et un maximum de 63 caractères ASCII imprimables.

Security Mode:	WPA Personal
WPA Algorithms:	TKIP
WPA Shared Key:	unmotclepourwpa
Group Key Renewal:	3600 seconds

Windows Zero Configuration

Il n'y a pratiquement pas de différence côté Windows entre la configuration WEP et la configuration WPA/WPA2 Personal si ce n'est que le réseau s'annonce cette fois-ci comme un réseau sécurisé WPA « Security-enabled wireless network (WPA) » et qu'il n'existe qu'une seule algorithmes pour obtenir la clé hexadécimale à partir du mot clé, ce qui vous permet d'utiliser celui-ci en toute tranquillité.



Attention : afin de pouvoir utiliser l'authentification à clé partagée, il faut aller dans la configuration avancé sans-fil du point d'accès et sélectionner « *shared key* »

De même, si vous voulez observer les trames CTS-to-self quand des stations 802.11b apparaissent dans le rayon de couverture du réseau, il faut activer la possibilité explicitement dans la fenêtre de paramétrage sans-fil avancée du point d'accès.