

CCNA Exploration - Commutation de réseau local et sans fil

Chapitre 7 – Concepts et Configuration de Base d'un Réseau sans Fil

7.0-Présentation du Chapitre

Dans les chapitres précédents, vous avez découvert en quoi les fonctions d'un commutateur peuvent faciliter l'interconnexion de périphériques sur un réseau filaire. Les réseaux d'entreprise types ont largement recours aux réseaux filaires. Des connexions physiques relient les systèmes informatiques, les systèmes téléphoniques et d'autres périphériques à des commutateurs situés dans les locaux techniques.

La gestion d'une infrastructure filaire peut être complexe. Réfléchissez aux implications d'une décision d'un employé qui souhaite déplacer un système informatique dans son bureau ou de la volonté d'un cadre d'amener un ordinateur portable en salle de réunion afin de l'y connecter au réseau. Dans un réseau filaire, cela implique dans le premier cas de tirer le câble de connexion réseau à un nouvel emplacement dans le bureau de l'employé et, dans le deuxième, de s'assurer qu'une connexion réseau est disponible dans la salle de réunion. C'est précisément pour éviter les contraintes de ce type que les réseaux sans fil tendent à se généraliser.

Dans ce chapitre, vous découvrirez en quoi les réseaux locaux sans fil (WLAN) offrent aux entreprises un environnement réseau flexible. Vous découvrirez les différentes normes sans fil actuellement disponibles, ainsi que les caractéristiques que chacune offre. Les composants matériels nécessaires pour constituer une infrastructure sans fil vous seront décrits, tout comme le fonctionnement des réseaux locaux sans fil et les moyens qui existent pour les sécuriser. Enfin, vous apprendrez à configurer un point d'accès sans fil et un client sans fil.

Dans ce chapitre, vous allez apprendre à effectuer les tâches suivantes :

- Décrire les composants et le fonctionnement de base des réseaux locaux sans fil
- Décrire les composants et le fonctionnement de la sécurité de base des réseaux locaux sans fil
- Configurer et vérifier l'accès de base aux réseaux locaux sans fil
- Résoudre les problèmes d'accès aux clients sans fil

7.1-Réseau Local Sans Fil

7.1.1-Pourquoi utiliser un Réseau Local sans fil

Page 1 :

Pourquoi les réseaux locaux sans fil ont-ils autant de succès ?

Cliquez sur le bouton de lecture dans la figure pour visualiser la vidéo.

Les réseaux d'entreprise d'aujourd'hui évoluent de façon à prendre en charge les personnes itinérantes. Qu'il s'agisse des salariés et des employeurs, des étudiants et des universités, des fonctionnaires et des usagers, des supporters de foot ou des consommateurs, tous sont mobiles et beaucoup d'entre eux sont « connectés ». Vous-même peut-être possédez-vous un téléphone portable vers lequel vous acheminez les messages instantanés lorsque vous êtes en déplacement sans votre ordinateur. C'est l'idée que l'on se fait de la mobilité : un environnement où les personnes peuvent faire suivre leur connexion réseau dans leurs déplacements.

Il existe divers types d'infrastructures (réseau local filaire, réseaux de fournisseurs de services) qui permettent de bénéficier d'une telle mobilité, mais dans un environnement d'entreprise, la plus importante est celle constituée par le réseau local sans fil.

La productivité ne se limite plus à un lieu de travail précis ou à une période définie. Désormais, les personnes jugent naturel d'être connectées en permanence et en tous lieux, du bureau à l'aéroport, voire même à domicile. Autrefois, les salariés itinérants étaient

contraints de passer des appels téléphoniques payants pour vérifier les messages et retourner des appels entre deux vols. À présent, les salariés peuvent consulter leurs courriels, leurs messages vocaux et l'état des produits sur leur assistant numérique personnel (PDA) sur leurs divers lieux de passage.

Chez les particuliers, nombreux sont ceux qui ont changé leur façon de vivre et de s'informer. L'Internet est devenu un service incontournable dans bon nombre de foyers, au même titre que la télévision ou le téléphone. Même le mode d'accès à Internet a rapidement évolué, passant d'un service commuté par modem temporaire à un service DSL ou câble dédié. Pour la souplesse qu'elles offrent, les particuliers recherchent des solutions sans fil comparables à celles dont bénéficient les employés de bureau. Pour la première fois, en 2005, il s'est vendu davantage d'ordinateurs portables Wi-Fi que d'ordinateurs de bureau fixes.

Outre la souplesse qu'ils procurent, les réseaux locaux sans fil offrent un avantage important en termes de coûts. Par exemple, lorsqu'une infrastructure sans fil est déjà en place, il est moins coûteux de déplacer une personne dans un bâtiment, de réorganiser un atelier ou d'effectuer un déménagement dans des locaux temporaires ou sur un site dans le cadre d'un projet. En termes de coûts informatiques, le fait de déménager un salarié sur un même site s'élève en moyenne à 250 euros.

Prenons maintenant l'exemple d'une société qui déménage dans un nouveau bâtiment sans aucune infrastructure filaire. Dans ce cas, les économies résultant de l'utilisation de réseaux locaux sans fil peuvent s'avérer encore plus spectaculaires dans la mesure où le coût que représente le fait de faire passer des câbles à travers les murs, les plafonds et les planchers est en grande partie écarté.

Bien que cela soit plus difficile à quantifier, les réseaux locaux sans fil peuvent avoir un effet favorable sur la productivité et le bien-être des salariés, ce qui peut profiter aux clients et aux résultats financiers de l'entreprise.

Page 2 :

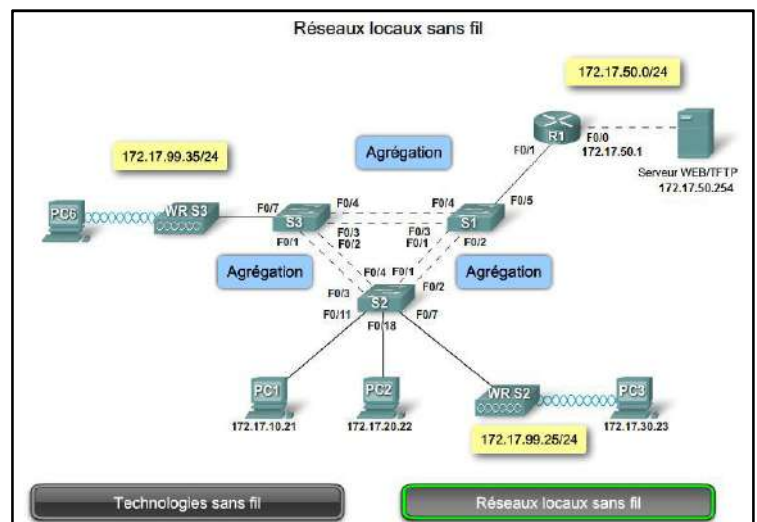
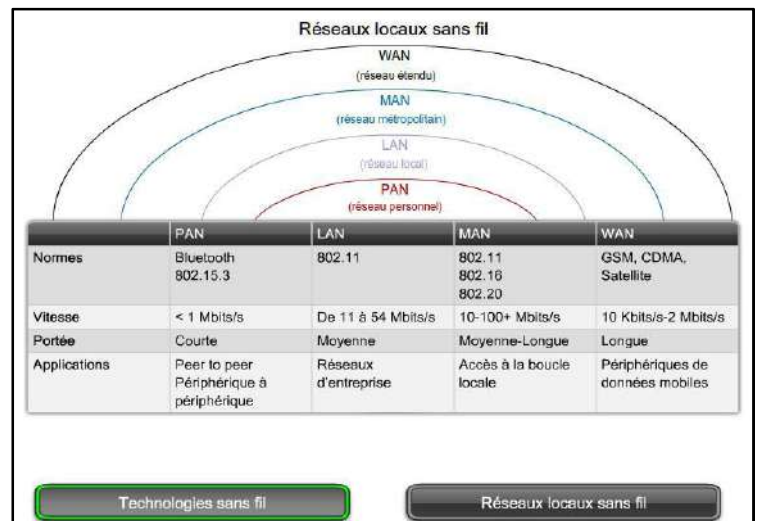
Réseaux locaux sans fil

Dans les chapitres précédents, vous avez découvert les technologies et les fonctions de commutation. La plupart des réseaux d'entreprise actuels reposent sur des réseaux locaux avec commutateurs pour les opérations quotidiennes à l'intérieur du bureau. Toutefois, les employés, de plus en plus mobiles, entendent pouvoir accéder aux ressources LAN de l'entreprise ailleurs que depuis leur propre bureau. Les employés sédentaires souhaitent pouvoir emmener leur ordinateur portable aux réunions ou dans le bureau d'un collègue. Lorsqu'il s'agit d'utiliser un ordinateur portable dans un autre lieu, compter sur une connexion filaire est une source de désagrément. Dans cette rubrique, vous découvrirez plus en détail les réseaux locaux sans fil (WLAN) et les avantages qu'ils confèrent à une entreprise. Vous explorerez également les problèmes de sécurité associés aux réseaux locaux sans fil.

La mobilité en matière de communications est devenue une attente partagée dans de nombreux pays du monde entier. La portabilité et la mobilité sont présentes dans tous les domaines, des claviers et casques sans fil aux téléphones satellitaires et systèmes de positionnement mondial (GPS). Combiner des technologies sans fil sur différents types de réseaux est un gage de mobilité pour les employés.

Cliquez sur le bouton Réseaux locaux sans fil dans la figure.

Comme vous pouvez le constater, le réseau local sans fil est une extension du réseau local Ethernet. Le réseau local a évolué pour devenir mobile. Vous allez découvrir la technologie du réseau local sans fil et les normes sur lesquelles repose la mobilité, qui permet à une personne de poursuivre une réunion pendant qu'elle se déplace dans la rue, en taxi ou à l'aéroport.



Page 3 :

Comparaison entre un réseau local sans fil et un réseau local filaire

Les réseaux locaux sans fil et les réseaux locaux Ethernet ont la même origine. L'IEEE a adopté l'ensemble de normes d'architecture de réseau informatique 802 LAN/MAN. Les deux principaux groupes de travail 802 sont ceux du réseau local Ethernet 802.3 et du réseau local sans fil IEEE 802.11. Toutefois, il existe des différences importantes entre les deux.

Les réseaux locaux sans fil utilisent des radiofréquences (RF) et non des câbles au niveau de la couche physique et de la sous-couche MAC de la couche liaison de données. Par rapport au câble, les radiofréquences présentent les caractéristiques suivantes :

- Contrairement aux fils gainés, les radiofréquences n'ont pas de limites. Du fait de cette absence de limites, les trames de données peuvent transiter au-delà des supports RF et être exploitées par quiconque pouvant recevoir le signal RF.
- Les radiofréquences ne sont pas protégées des signaux extérieurs, à la différence des câbles qui sont enveloppés d'une gaine isolante. Autrement dit, les radios fonctionnant de manière indépendante sur un même secteur géographique mais qui utilisent des radiofréquences identiques ou similaires peuvent interférer entre elles.
- La transmission RF est sujette aux difficultés inhérentes aux technologies reposant sur les ondes, comme les radios grand public. Par exemple, à mesure que vous vous éloignez de la source, vous pouvez entendre plusieurs stations se chevaucher ou bien des grésillements au niveau de la transmission. Vous pouvez même finir par perdre tout signal. Les réseaux locaux filaires sont équipés de câbles de longueur appropriée pour éviter que le signal ne perde en intensité.
- La réglementation concernant les bandes RF peut être différente d'un pays à un autre. L'utilisation de réseaux locaux sans fil est soumise à d'autres réglementations et ensembles de normes qui ne s'appliquent pas aux réseaux locaux filaires.

Dans un environnement de réseau local sans fil, les clients sont connectés au réseau par le biais non pas d'un commutateur Ethernet mais d'un point d'accès sans fil.

Les périphériques connectés aux réseaux locaux sans fil sont généralement des appareils mobiles alimentés par batteries, au contraire des périphériques LAN qui sont branchés sur secteur. Les cartes réseau sans fil tendent à réduire l'autonomie d'un périphérique mobile.

Les réseaux locaux sans fil prennent en charge les hôtes qui rivalisent pour accéder aux supports RF (bandes de fréquences). L'ensemble de normes 802.11 prescrit l'évitement de collision plutôt que la détection de collision pour l'accès aux supports de façon à éviter par anticipation les collisions à l'intérieur des supports.

Les réseaux locaux sans fil utilisent un format de trame différent de celui des réseaux locaux Ethernet filaires. Les réseaux locaux sans fil ont besoin d'informations supplémentaires au niveau de l'en-tête de couche 2 de la trame.

Les réseaux locaux sans fil posent davantage de problèmes en matière de confidentialité dans la mesure où les fréquences radio peuvent atteindre l'extérieur.

Page 4 :

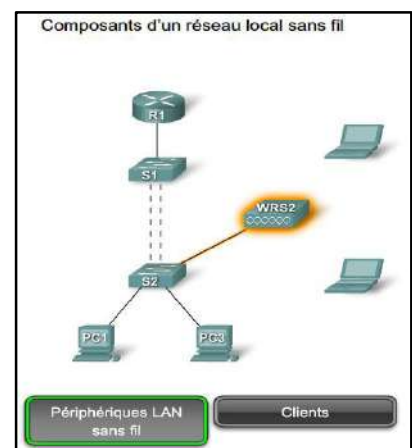
Présentation des réseaux locaux sans fil

Les réseaux locaux sans fil 802.11 constituent une extension des infrastructures LAN Ethernet 802.3 qui vise à offrir des options de connectivité supplémentaires. Cependant, des composants et des protocoles supplémentaires sont utilisés pour établir des connexions sans fil.

Dans un réseau local Ethernet répondant à la norme 802.3, chaque client est muni d'un câble qui vient relier sa carte réseau à un commutateur. Pour le client, le commutateur représente le point d'accès au réseau.

Cliquez sur le bouton Périphériques LAN sans fil dans la figure.

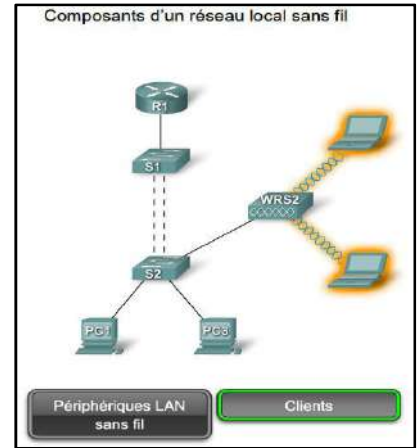
Caractéristique	Réseau local sans fil 802.11	Réseaux locaux Ethernet 802.3
Couche physique	Radiofréquence (RF)	Câble
Accès aux supports	Évitement de collision	Détection de collisions
Disponibilité	Quiconque équipé d'une carte réseau radio dans la portée d'émission d'un point d'accès	Connexion par câble requise
Signaux parasites	Oui	Sans conséquence
Réglementation	Autres réglementations édictées par les autorités locales	Norme IEEE



Dans un réseau local sans fil, chaque client utilise une carte réseau sans fil pour accéder au réseau via un périphérique sans fil tel qu'un routeur ou un point d'accès sans fil.

Cliquez sur le bouton Clients dans la figure.

La carte réseau sans fil dont est équipé le client communique avec le routeur ou le point d'accès sans fil par le biais de signaux RF. Une fois connectés au réseau, les clients sans fil peuvent accéder aux ressources réseau comme s'ils étaient reliés au réseau par câble.



7.1.2-Normes des Réseaux Locaux Sans Fil

Page 1 :

Normes des réseaux locaux sans fil

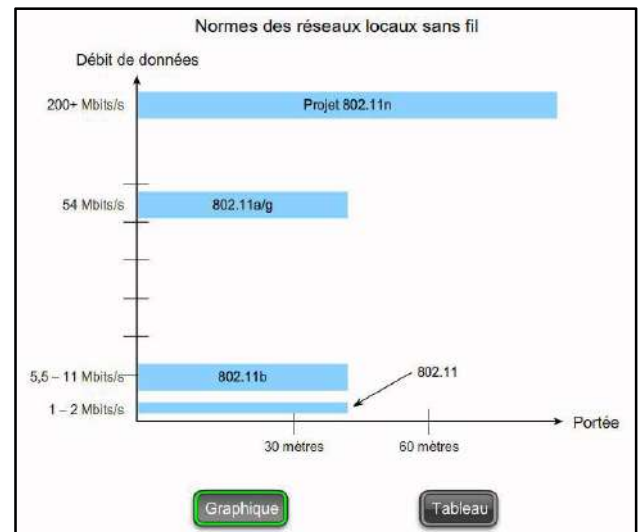
La norme 802.11 relative aux réseaux locaux sans fil est une norme IEEE qui définit la façon dont les radiofréquences (RF) dans les bandes de fréquences ISM (industrielles, scientifiques et médicales) sans licence sont utilisées pour la couche physique et la sous-couche MAC des liaisons sans fil.

Au moment de sa publication initiale, la norme 802.11 prescrivait des débits de données compris entre 1 et 2 Mbits/s dans la bande 2,4 GHz. À cette époque, les réseaux locaux sans fil fonctionnaient à 10 Mbits/s, si bien que la nouvelle technologie sans fil ne fut pas accueillie avec enthousiasme. Depuis, les normes relatives aux réseaux locaux sans fil se sont constamment améliorées avec la publication des normes IEEE 802.11a, IEEE 802.11b, IEEE 802.11g et le projet de norme 802.11n.

En règle générale, le choix de la norme WLAN se fait en fonction des débits de données. Par exemple, les normes 802.11a et g peuvent prendre en charge un débit maximal de 54 Mb/s, tandis que la norme 802.11b prend en charge jusqu'à 11 Mbits/s, ce qui fait de 802.11b la norme « lente » et 802.11 a et g les normes préférées. Une quatrième norme WLAN à l'état de projet, 802.11n, dépasse les débits de données actuellement disponibles. La norme IEEE 802.11n devrait être ratifiée d'ici septembre 2008. La figure compare les normes ratifiées IEEE 802.11a, b et g.

Cliquez sur le bouton Tableau dans la figure pour afficher des détails sur chaque norme.

Les débits de données des différentes normes de réseaux locaux sans fil sont affectés par ce que l'on appelle une technique de modulation. Les deux techniques de modulation dont il est question dans ce cours sont les techniques DSSS (Direct Sequence Spread Spectrum ou étalement du spectre en séquence directe) et OFDM (Orthogonal Frequency Division Multiplexing ou multiplexage par répartition orthogonale de la fréquence). S'il ne vous est pas demandé de connaître le fonctionnement de ces techniques dans le cadre de ce cours, vous devez toutefois savoir que lorsqu'une norme utilise la technique OFDM, les débits de données qu'elle offre sont plus élevés. De même, sachez que la technique DSSS est plus simple que la technique OFDM et donc moins coûteuse à mettre en œuvre.



	802.11a	802.11b	802.11g	802.11n
Bande	5,7 GHz	2,4 GHz	2,4 GHz	À confirmer Bandes 2,4 et 5 GHz (probablement)
Canaux*	Jusqu'à 23	3	3	
Modulation	OFDM	DSSS	DSSS	OFDM
Débits de données	Jusqu'à 54 Mbits/s	Jusqu'à 11 Mbits/s	Jusqu'à 11 Mbits/s	Jusqu'à 54 Mbits/s
Avantages	~35 mètres	~35 mètres	~35 mètres	~70 mètres
Inconvénients	Octobre 1999	Octobre 1999	Juin 2003	Ratification attendue en 2008
Avantages	Rapidité, moins sujette aux interférences	Faible coût, bonne portée	Rapidité, bonne portée, peu sensible aux obstacles	Excellents débits de données, portée accrue
Inconvénients	Coût plus élevé, portée inférieure	Lent, sujette aux interférences	Sujette aux interférences des appareils utilisant la bande 2,4 GHz	

* Canaux sans chevauchement

Graphique

Tableau

802.11a

La norme IEEE 802.11a a adopté la technique de modulation OFDM et utilise la bande 5 GHz.

Les périphériques 802.11a fonctionnant dans la bande 5 GHz présentent moins de risques de subir des interférences que les périphériques qui fonctionnent dans la bande 2,4 GHz, car les appareils grand public qui utilisent la bande 5 GHz sont moins nombreux. Par ailleurs, les fréquences élevées autorisent l'utilisation d'antennes plus petites.

L'utilisation de la bande 5 GHz présente plusieurs inconvénients de taille. En premier lieu, les ondes radio de haute fréquence sont plus facilement absorbées par les obstacles tels que les murs, ce qui rend davantage la norme 802.11a prédisposée à de mauvaises performances en cas d'obstacles. En second lieu, cette bande à hautes fréquences offre une portée sensiblement plus faible que la norme 802.11b ou g. Par ailleurs, certains pays, comme la Russie, n'autorisent pas l'utilisation de la bande 5 GHz, ce qui risque de limiter un peu plus son déploiement.

802.11b et 802.11g

Selon la norme 802.11b, les débits de données spécifiés dans la bande ISM 2,4 GHz sont de 1, 2, 5,5 et 11 Mbits/s avec la technique DSSS. La norme 802.11g assure des débits de données plus élevés dans cette bande en utilisant la technique de modulation OFDM. De plus, la norme IEEE 802.11g prévoit l'utilisation de la technique DSSS pour assurer une compatibilité en amont avec les systèmes IEEE 802.11b. Les débits de données DSSS de 1, 2, 5,5 et 11 Mbits/s sont pris en charge, tout comme les débits de données OFDM de 6, 9, 12, 18, 24, 48 et 54 Mbits/s.

Il existe des avantages à utiliser la bande 2,4 GHz. Ainsi, les périphériques qui utilisent la bande 2,4 GHz disposent d'une meilleure plage que ceux qui utilisent la bande 5 GHz. De même, les transmissions dans cette bande ne sont pas aussi sensibles aux obstacles qu'avec la norme 802.11a.

L'utilisation de la bande 2,4 GHz présente un inconvénient non négligeable. Bon nombre d'appareils grand public utilisent également la bande 2,4 GHz, ce qui a pour effet d'exposer les appareils 802.11b et g à des perturbations.

802.11n

Le projet de norme IEEE 802.11n vise à améliorer les débits de données et la portée des réseaux locaux sans fil sans pour autant faire appel à une puissance supplémentaire ou à une attribution de bande RF. Le projet de norme 802.11n prévoit l'utilisation de plusieurs radios et antennes aux extrémités, chacune diffusant sur la même fréquence pour établir plusieurs flux. La technologie MIMO (entrée multiple/sortie multiple) décompose un flux à haut débit de données en plusieurs flux de débit inférieur et les diffuse simultanément sur les radios et les antennes disponibles. Cela permet d'obtenir un débit de données théorique maximal de 248 Mbits/s en utilisant deux flux.

La norme devrait être ratifiée d'ici septembre 2008.

Important : les bandes RF sont attribuées par l'ITU-R (Union Internationale des Télécommunications secteur de normalisation des Télécommunications). L'ITU-R considère que les bandes de fréquences 900 MHz, 2,4 GHz et 5 GHz sont sans licence pour les communautés ISM. Bien que les bandes ISM soient sans licence à l'échelle planétaire, elles demeurent soumises à des réglementations locales. L'utilisation de ces bandes est gérée par la FCC aux États-Unis et par l'ETSI en Europe. Ces éléments auront une influence sur votre sélection de composants sans fil dans le cadre de la mise en œuvre d'un réseau sans fil.

Page 2 :

Certification Wi-Fi

La certification Wi-Fi est délivrée par la Wi-Fi Alliance (<http://www.wi-fi.org>). L'objet de cette association professionnelle à but non lucratif est de favoriser le développement et l'adoption des réseaux locaux sans fil. Vous comprendrez mieux l'importance de la certification Wi-Fi si vous considérez le rôle de la Wi-Fi Alliance dans le contexte des normes des réseaux locaux sans fil.

Les normes assurent une interopérabilité entre les périphériques produits par différents fabricants. Sur le plan international, les trois organismes ayant le plus de poids au niveau des normes des réseaux locaux sans fil sont les suivants :

- ITU-R
- IEEE
- Wi-Fi Alliance

L'ITU-R édicte des règles concernant l'attribution du spectre de radiofréquences et les orbites satellitaires. Celles-ci sont décrites comme étant des ressources naturelles finies dont la demande émane de consommateurs tels que les réseaux sans fil fixes, les réseaux sans fil mobiles et les systèmes GPS.

L'IEEE a élaboré et adapte les normes applicables aux réseaux locaux et métropolitains (famille de normes IEEE 802 LAN/MAN). L'ensemble de normes IEEE 802 est géré par le comité de normes IEEE 802 LAN/MAN (LMSC), qui supervise les divers groupes de travail. Les normes dominantes de la famille IEEE 802 sont les normes 802.3 Ethernet, 802.5 Token Ring et 802.11 Wireless LAN.

Bien que l'IEEE ait spécifié des normes pour les appareils de modulation de radiofréquences, elle n'a pas spécifié de normes de fabrication, si bien que les interprétations discordantes des normes 802.11 faites par les différents fournisseurs peuvent être à l'origine de problèmes d'interopérabilité entre leurs appareils.

Certification Wi-Fi



La Wi-Fi Alliance est une association de fournisseurs dont l'objectif est d'améliorer l'interopérabilité des produits reposant sur la norme 802.11 en certifiant les fournisseurs qui se conforment et s'en tiennent aux normes de l'industrie. La certification porte non seulement sur les trois technologies de radiofréquence IEEE 802.11, mais également sur les projets de norme IEEE en anticipation de leur adoption, comme 802.11n et les normes de sécurité WPA et WPA2 qui reposent sur la norme IEEE 802.11i.

Le rôle de ces trois organisations peut être résumé ainsi :

- L'ITU-R régit l'attribution des bandes RF.
- L'IEEE spécifie la façon dont les radiofréquences sont modulées pour la transmission des informations.
- La Wi-Fi Alliance s'assure que les fournisseurs fabriquent des périphériques interopérables.

7.1.3-Composants d'une Infrastructure sans fil

Page 1 :

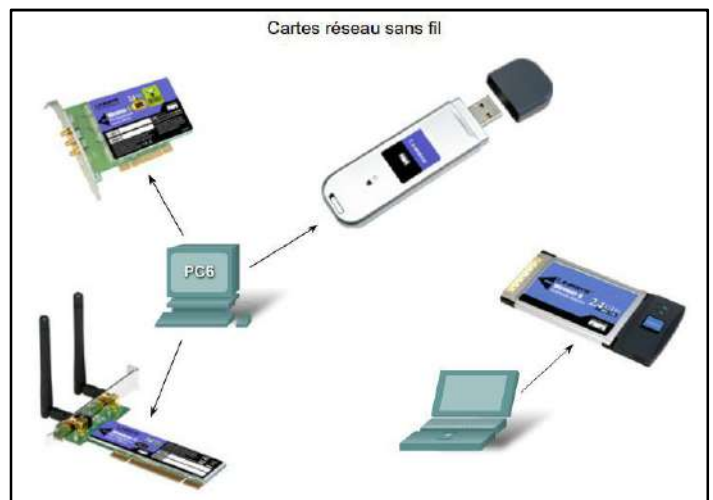
Cartes réseau sans fil

Il se peut que vous utilisiez déjà un réseau sans fil à domicile, dans un café en bas de chez vous ou dans l'établissement que vous fréquentez. Vous êtes-vous déjà posé la question de savoir quels sont les composants matériels qui vous permettent d'accéder sans fil au réseau local ou à Internet ? Dans cette rubrique, vous allez découvrir les différents composants susceptibles d'intervenir dans la mise en œuvre d'un réseau local sans fil et la façon dont chacun est utilisé dans une infrastructure sans fil.

Pour rappel, un réseau local sans fil est constitué pour l'essentiel de stations client qui se connectent à des points d'accès qui, à leur tour, se connectent à l'infrastructure réseau. Le périphérique qui permet à une station client d'envoyer et recevoir des signaux RF est la carte réseau sans fil.

À l'instar d'une carte réseau Ethernet, la carte réseau sans fil code un flux de données sur un signal RF selon la technique de modulation définie. Les cartes réseau sans fil sont le plus souvent associées à des périphériques mobiles, tels que des ordinateurs portables. Dans les années 1990, les cartes réseau sans fil pour ordinateurs portables étaient des cartes que l'on logeait dans un emplacement PCMCIA. Bien que les cartes réseau sans fil PCMCIA soient toujours monnaie courante, nombreux sont les fabricants qui ont commencé à équiper les ordinateurs portables de cartes réseau sans fil. À la différence des interfaces Ethernet 802.3 intégrées aux PC, la carte réseau sans fil n'est pas visible puisqu'il n'est pas nécessaire d'y connecter un câble.

Par ailleurs, d'autres options ont vu le jour au fil des ans. Les ordinateurs de bureau situés dans une installation sans fil existante peuvent être équipés d'une carte réseau sans fil PCI. Pour installer rapidement un PC, portable ou fixe, muni d'une carte réseau sans fil, il existe également de nombreuses options USB.



Page 2 :

Points d'accès sans fil

Un point d'accès permet de relier des clients sans fil (ou stations) à un réseau local filaire. En règle générale, les périphériques client ne communiquent pas directement entre eux ; ils communiquent avec le point d'accès. En substance, un point d'accès convertit les paquets de données TCP/IP, les faisant passer de leur format d'encapsulation de trames radio 802.11 au format de trame Ethernet 802.3 sur le réseau Ethernet filaire.

Dans un réseau d'infrastructure, les clients doivent être associés à un point d'accès pour pouvoir bénéficier de services réseau. Pour un client, l'association est le processus qui consiste à se joindre à un réseau 802.11. Cela revient à se brancher sur un réseau local filaire. Le processus d'association est décrit ultérieurement.

Un point d'accès est un périphérique de couche 2 qui fonctionne comme un concentrateur Ethernet 802.3. Les radiofréquences constituent un support partagé et les points d'accès sont à l'écoute de l'ensemble du trafic radio. À l'image des périphériques Ethernet 802.3, les périphériques qui souhaitent utiliser le support se font concurrence. Toutefois, contrairement aux cartes réseau Ethernet, il est coûteux de fabriquer des cartes réseau sans fil qui puissent à la fois transmettre et recevoir des données, si bien que les périphériques radio ne détectent pas les collisions. Au lieu de cela, les périphériques de réseau local sans fil sont conçus pour les éviter.

CSMA/CA

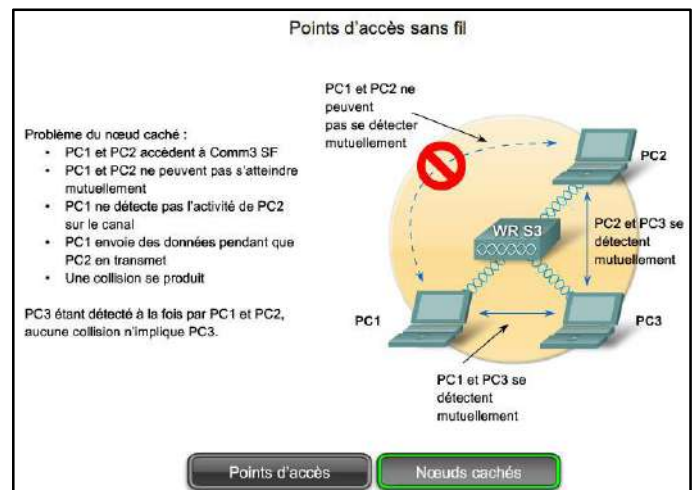
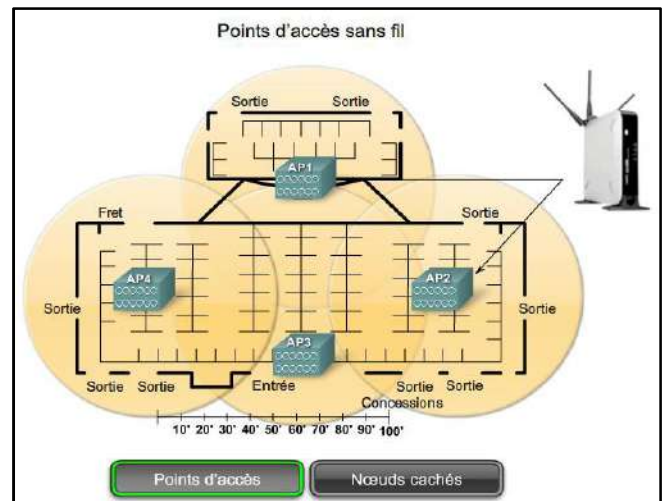
Les points d'accès supervisent une fonction de coordination répartie appelée CSMA/CA (accès multiple avec écoute de porteuse avec évitement de collision). Cela veut simplement dire que les périphériques d'un réseau local sans fil doivent capter l'énergie au niveau du support (stimulation par radiofréquence au-dessus d'un certain seuil) et attendre que le support soit disponible avant de procéder à l'envoi. Tous les périphériques étant tenus d'opérer de la sorte, la fonction de coordination de l'accès au support est répartie. Si un point d'accès reçoit des données en provenance d'une station client, il lui envoie un reçu pour accuser réception des données. Ce reçu vise à informer le client qu'aucune collision ne s'est produite et à l'empêcher de retransmettre les données.

Cliquez sur le bouton *Nœuds cachés* dans la figure.

Les signaux RF s'atténuent. Cela signifie qu'ils perdent en intensité à mesure qu'ils s'éloignent de leur point d'origine. C'est à l'image de ce qu'il se passe lorsque, en voiture, vous perdez le signal d'une station radio. Cette atténuation du signal peut être un problème dans un réseau local sans fil lorsque les stations rivalisent pour l'accès au support.

Imaginez le cas de deux stations client qui se connectent toutes deux à un même point d'accès, mais qui se trouvent de part et d'autre de celui-ci. Si la distance qui les sépare du point d'accès correspond à la portée maximale, elles ne pourront pas s'atteindre mutuellement. Autrement dit, ni l'une ni l'autre des deux stations ne captera l'autre sur le support, et elles risquent en fin de compte de transmettre simultanément. C'est ce que l'on appelle le problème du nœud (ou station) caché.

Un moyen de résoudre le problème du nœud caché est de recourir à une fonction CSMA/CA appelée Demande pour émettre/Prêt à émettre (DPE/PAE). La fonction DPE/PAE a été développée afin de permettre une négociation entre un client et un point d'accès. Lorsque la fonction DPE/PAE est activée dans un réseau, les points d'accès affectent le support à la station demandeuse le temps qu'il faut pour terminer la transmission. Lorsque la transmission est terminée, les autres stations peuvent demander le canal de la même façon. Sinon, la fonction normale d'évitement de collision est rétablie.

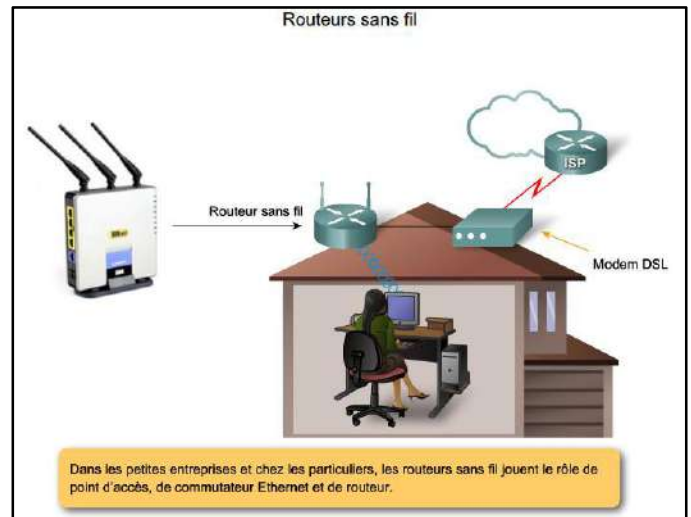


Page 3 :

Routeurs sans fil

Les routeurs sans fil jouent le rôle de point d'accès, de commutateur Ethernet et de routeur. Par exemple, le périphérique Linksys WRT300N utilisé est bel et bien un appareil « trois en un ». Il se compose tout d'abord d'un point d'accès sans fil, qui assure les fonctions classiques d'un point d'accès ; ensuite, d'un commutateur intégré 10/100 bidirectionnel simultané à quatre ports, qui fournit une connectivité aux périphériques filaires ; et enfin, d'une fonction de routeur, qui procure une passerelle pour se connecter aux autres infrastructures réseau.

Le WRT300N est généralement utilisé chez les particuliers ou dans des petites entreprises en tant que périphérique d'accès sans fil. La charge attendue au niveau du périphérique étant suffisamment faible, il doit être en mesure de gérer le service de réseau local sans fil, 802.3 Ethernet, et de se connecter à un fournisseur de services Internet.



7.1.4-Fonctionnement sans fil

Page 1 :

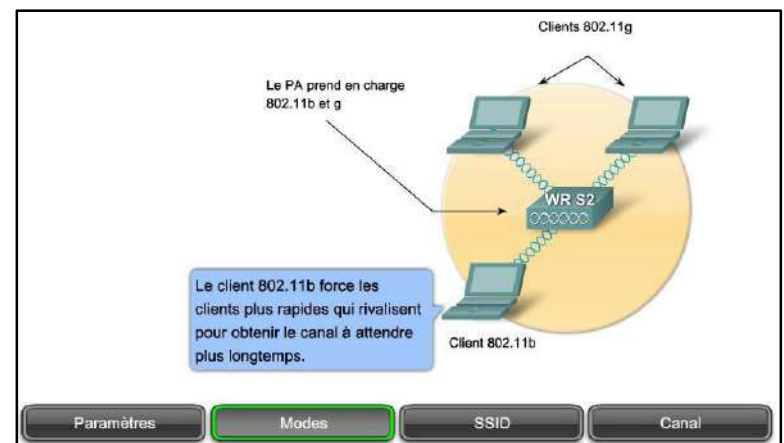
Paramètres configurables pour les points d'extrémité sans fil

La figure présente l'écran initial de configuration sans fil d'un routeur sans fil Linksys. La création d'une connexion entre un client et un point d'accès implique plusieurs processus. Vous devez configurer les paramètres sur le point d'accès (et par la suite sur votre périphérique client) pour permettre la négociation de ces processus.



Cliquez sur le bouton Modes dans la figure pour consulter le paramètre Wireless Network Mode.

Le paramètre Wireless Network Mode (Mode réseau sans fil) fait référence aux protocoles de réseau local sans fil suivants : 802.11a, b, g ou n. Le protocole 802.11g étant compatible en amont avec 802.11b, les points d'accès prennent en charge les deux normes. Ne perdez pas de vue que si tous les clients se connectent à un point d'accès conformément à la norme 802.11g, ils bénéficient tous des meilleurs débits de données disponibles. Lorsque des clients 802.11b s'associent au point d'accès, tous les clients rapides qui rivalisent pour obtenir le canal doivent attendre que les clients 802.11b aient libéré le canal avant de transmettre. Lorsqu'un point d'accès Linksys est configuré pour autoriser les clients 802.11b et 802.11g, il fonctionne en mode mixte.



Pour permettre à un point d'accès de prendre en charge 802.11a, ainsi que 802.11b et g, il doit disposer d'une seconde radio pour fonctionner dans l'autre bande RF.

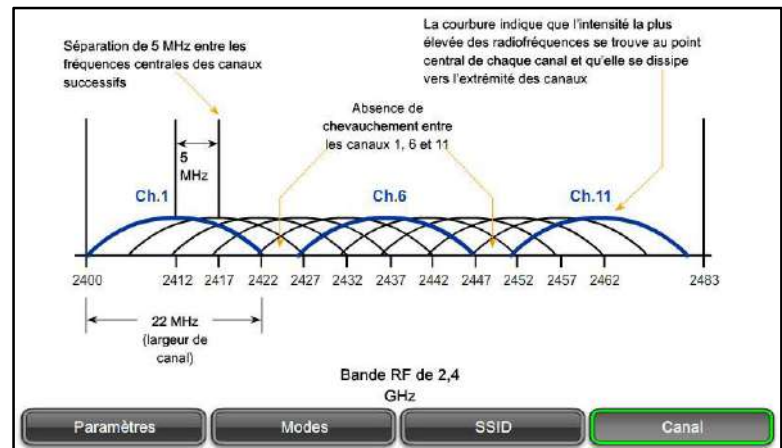
Cliquez sur le bouton SSID dans la figure pour afficher la liste de SSID d'un client Windows.

Un identificateur d'ensemble de services partagé (SSID) est un identificateur unique qu'utilisent les périphériques client pour distinguer plusieurs réseaux sans fil dans un même voisinage. Un SSID peut être partagé par plusieurs points d'accès sur un même réseau. La figure illustre un exemple de SSID permettant de distinguer plusieurs réseaux locaux sans fil. Les SSID peuvent correspondre à une entrée alphanumérique, sensible à la casse, constituée de 2 à 32 caractères.



Cliquez sur le bouton Canal dans la figure pour afficher un graphique de canaux sans chevauchement.

La norme IEEE 802.11 établit le modèle de découpage en canaux pour l'utilisation des bandes RF ISM sans licence dans les réseaux locaux sans fil. La bande 2,4 GHz est découpée en 11 canaux pour l'Amérique du Nord et en 13 canaux pour l'Europe. La fréquence centrale de ces canaux est séparée de seulement 5 MHz et leur bande passante globale (ou occupation de fréquence) est de 22 MHz. Une bande passante de canal de 22 MHz combinée à une séparation de 5 MHz entre les fréquences centrales signifie qu'il existe un chevauchement entre les canaux successifs. Or, dans le cas des réseaux locaux sans fil qui nécessitent plusieurs points d'accès, les Méthodes Recommandées préconisent l'utilisation de canaux sans chevauchement. S'il existe trois points d'accès adjacents, utilisez les canaux 1, 6 et 11. S'il n'en existe que deux, sélectionnez-en deux qui soient séparés de cinq canaux (p. ex., les canaux 5 et 10). Bon nombre de points d'accès sont en mesure de sélectionner automatiquement un canal en fonction de l'utilisation de canaux adjacents. Certains produits surveillent constamment l'espace radio pour ajuster dynamiquement les paramètres des canaux en réponse aux changements intervenant dans l'environnement.



Page 2 :

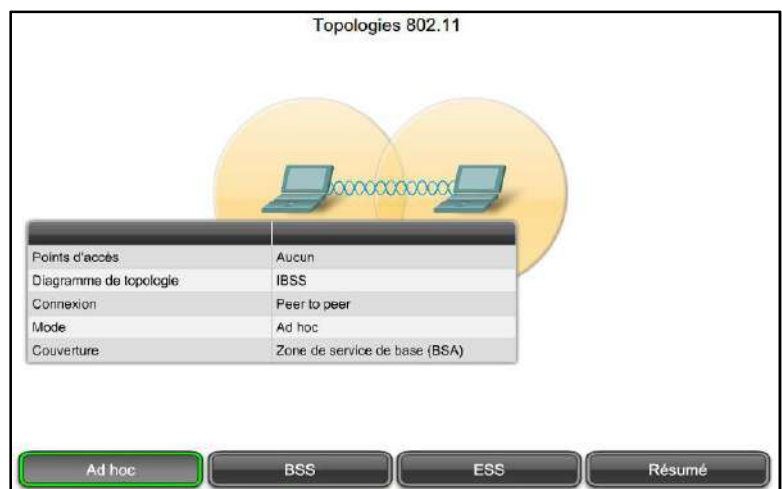
Topologies 802.11

Les réseaux locaux sans fil peuvent accueillir plusieurs topologies réseau. Dans la description de ces topologies, la pierre angulaire de l'architecture de réseau locaux sans fil IEEE 802.11 est l'ensemble de services de base (BSS). La norme définit l'ensemble de services de base comme un groupe de stations qui communiquent entre elles.

Cliquez sur le bouton Ad Hoc dans la figure.

Réseaux ad hoc

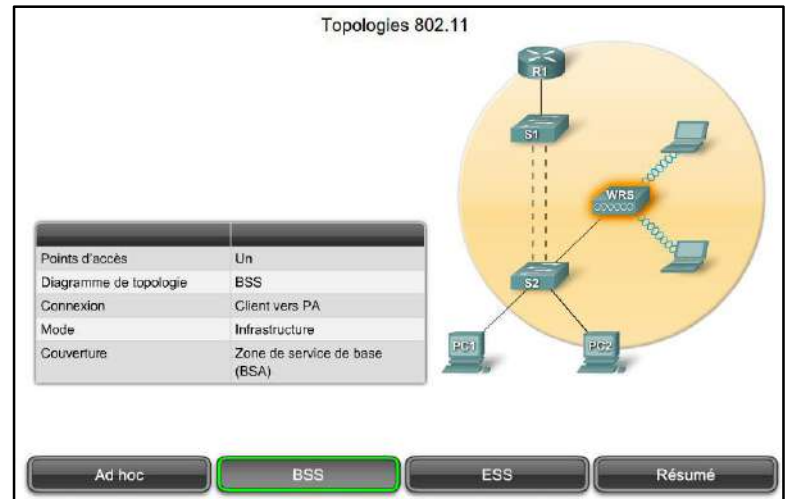
Les réseaux sans fil peuvent fonctionner sans points d'accès ; il s'agit dans ce cas d'une topologie ad hoc. Les stations client configurées pour fonctionner en mode ad hoc se configurent entre elles les paramètres sans fil. La norme IEEE 802.11 désigne un réseau ad hoc sous le nom IBSS (Independent BSS, ensemble de services de base indépendant).



Cliquez sur le bouton BSS dans la figure.

Ensembles de services de base

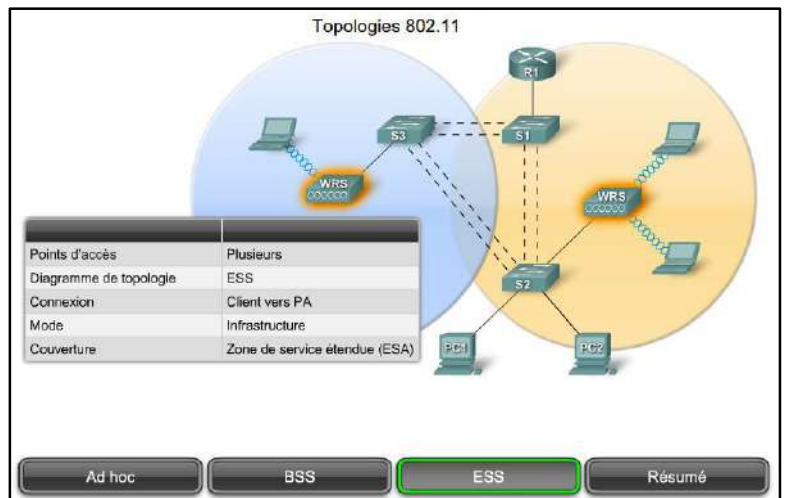
Les points d'accès procurent une infrastructure qui ajoute des services et améliore la portée des clients. Un seul point d'accès en mode infrastructure permet de gérer les paramètres sans fil et la topologie consiste simplement en un ensemble de services de base. La zone de couverture d'un IBSS et d'un BSS est appelée basic service area (BSA).



Cliquez sur le bouton ESS dans la figure.

Éventails de services étendus

Lorsqu'un ensemble de services de base n'assure pas une couverture en radiofréquences suffisante, un ou plusieurs ensembles de ce type peuvent être joints par le biais d'un système de distribution commun de manière à former un éventail de services étendu (ESS). Dans un ESS, un BSS se distingue d'un autre par son identificateur (BSSID), qui correspond à l'adresse MAC du point d'accès desservant le BSS. La zone de couverture est la zone de services étendue (Extended Service Area, ESA).

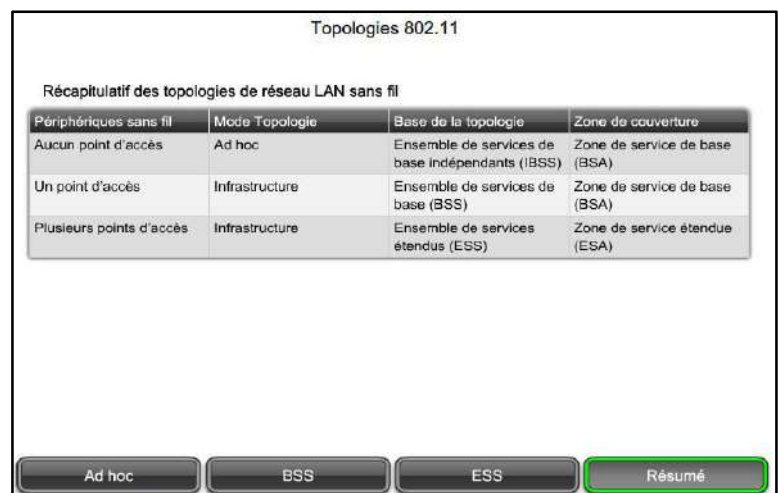


Système de distribution commun

Le système de distribution commun permet à plusieurs points d'accès au sein d'un ensemble de services étendus d'apparaître en tant qu'ensemble de services de base unique. En règle générale, un ensemble de services étendus comprend un SSID commun qui permet à un utilisateur de passer d'un point d'accès à un autre (« itinérance » ou « roaming »).

Les cellules représentent la zone de couverture fournie par un seul canal. Un ensemble de services étendus doit présenter un chevauchement de 10 à 15 % entre les cellules d'une zone de services étendue. Avec un chevauchement de 15 % entre les cellules, un SSID et des canaux sans chevauchement (une cellule sur le canal 1 et l'autre sur le canal 6), la fonctionnalité d'itinérance peut être créée.

Cliquez sur le bouton Résumé dans la figure pour obtenir une comparaison des topologies de réseau local sans fil.



Page 3 :

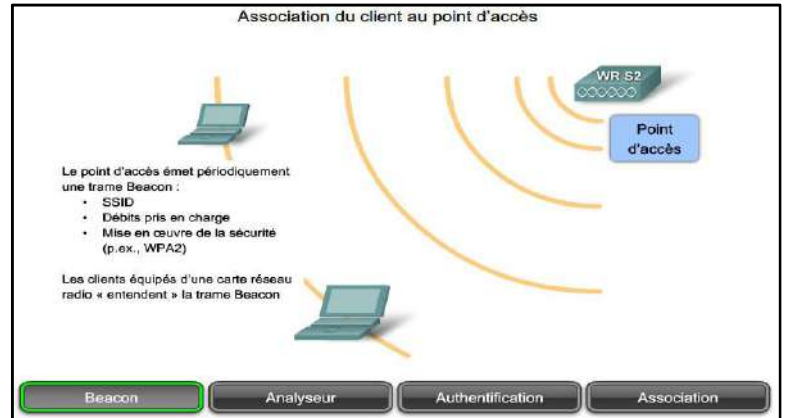
Association du client au point d'accès

L'une des principales étapes du processus 802.11 est celle qui consiste à découvrir un réseau local sans fil et ensuite à s'y connecter. Les principales composantes de ce processus sont les suivantes :

- Trames Beacon - Trames utilisées par le réseau local sans fil pour annoncer sa présence.
- Analyseurs - Trames utilisées par les clients des réseaux locaux sans fil pour trouver leur réseau.
- Authentification - Processus correspondant à un objet représentatif de la norme 802.11 d'origine mais qui reste exigé par la norme.
- Association - Processus visant à établir une liaison de données entre un point d'accès et un client de réseau local sans fil.

La trame Beacon vise essentiellement à permettre aux clients d'un réseau local sans fil de détecter les réseaux et les points d'accès disponibles dans une zone donnée, et donc de leur permettre de choisir quel réseau et quel point d'accès utiliser. Les points d'accès peuvent diffuser périodiquement des trames Beacon.

Si les trames Beacon peuvent être diffusées régulièrement par un point d'accès, il n'en est pas de même pour les trames d'analyse, d'authentification et d'association, qui ne sont utilisées que dans le cadre du processus d'association (ou de réassociation).



Processus d'association 802.11

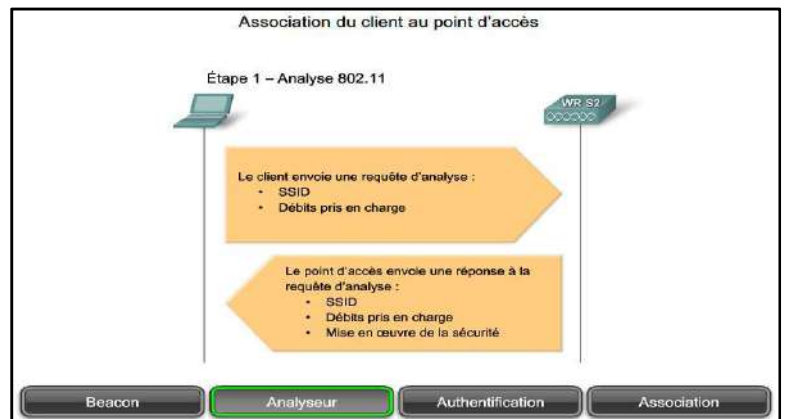
Avant de pouvoir envoyer des données sur un réseau local sans fil, un client 802.11 doit exécuter le processus en trois étapes suivant :

Cliquez sur le bouton Analyseur dans la figure.

Étape 1 – Analyse 802.11

Pour rechercher un réseau spécifique, les clients envoient une requête d'analyse sur plusieurs canaux. La requête d'analyse spécifie le nom du réseau (SSID) et les débits. Un client type de réseau local sans fil étant configuré avec un SSID déterminé, les requêtes d'analyse en provenance de ce client contiennent le SSID du réseau local sans fil souhaité.

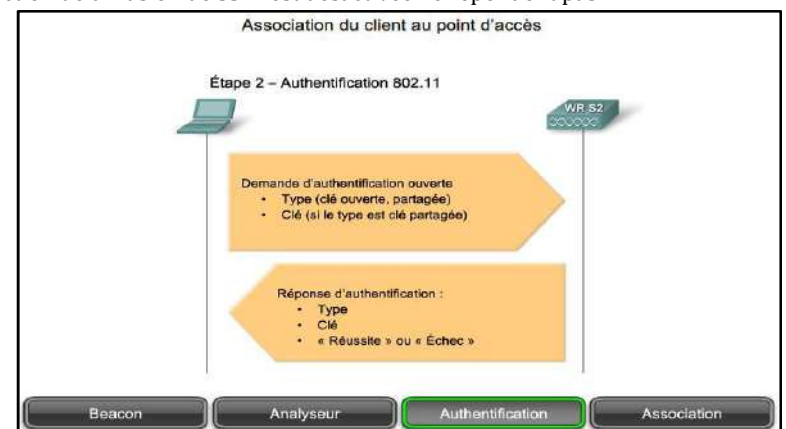
Si le client du réseau local sans fil tente simplement de découvrir les réseaux locaux sans fil disponibles, il peut envoyer une requête d'analyse sans SSID. Auquel cas, tous les points d'accès configurés pour répondre à ce type de requête émettent une réponse. En revanche, les réseaux locaux sans fil dont la fonction de diffusion de SSID est désactivée ne répondent pas.



Cliquez sur le bouton Authentification dans la figure.

Étape 2 – Authentification 802.11

À l'origine, la norme 802.11 fut développée avec deux mécanismes d'authentification. Le premier, appelé authentification ouverte, consiste essentiellement en une authentification NULL où le client émet le message « authentifie-moi », auquel le point d'accès répond « oui ». Il s'agit du mécanisme utilisé dans pratiquement tous les déploiements de 802.11.

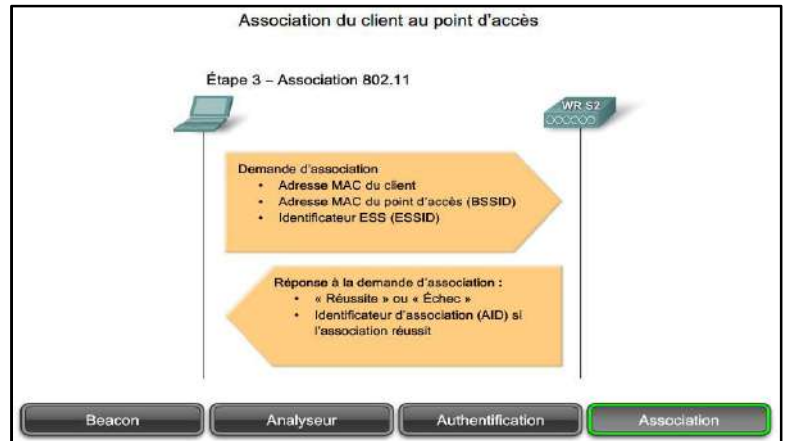


Le second mécanisme d'authentification est basé sur une clé partagée entre la station client et le point d'accès appelée clé WEP (Wired Equivalency Protection). Le principe de la clé WEP partagée est qu'elle confère à une liaison sans fil un niveau de confidentialité équivalent à celui d'une liaison filaire. Or, la mise en œuvre initiale de cette méthode d'authentification était défectueuse. Pour être conformes aux normes, les mises en œuvre de clients et de points d'accès doivent intégrer l'authentification par clé partagée. Toutefois, elle n'est ni utilisée, ni recommandée.

Cliquez sur le bouton Association dans la figure.

Étape 3 – Association 802.11

Cette étape vise à valider les options de sécurité et de débit et à établir la liaison de données entre le client de réseau local sans fil et le point d'accès. Au cours de cette étape, le client apprend le BSSID, qui correspond à l'adresse MAC du point d'accès, lequel mappe un port logique connu en tant qu'identificateur d'association (Association Identifier, AID) sur le client de réseau local sans fil. L'AID équivaut à un port de commutateur. Le processus d'association permet au commutateur de l'infrastructure d'effectuer le suivi des trames destinées au client WLAN pour qu'elles puissent être réacheminées.



Dès lors qu'un client WLAN est associé à un point d'accès, un échange de trafic peut alors avoir lieu entre ces deux périphériques.

7.1.5-Planification du réseau local sans fil

Page 1 :

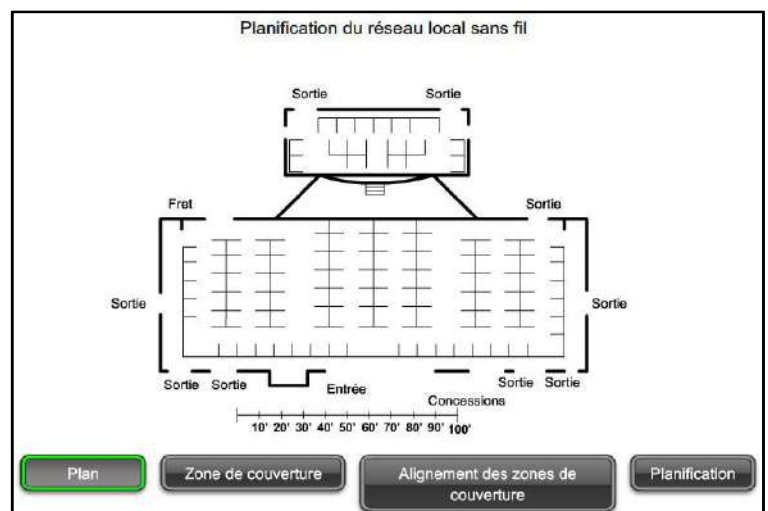
Planification du réseau local sans fil

La mise en œuvre d'un réseau local sans fil qui exploite au mieux les ressources et assure un niveau de service optimal peut nécessiter une planification soigneuse. Les réseaux locaux sans fil peuvent aller d'installations relativement simples à des conceptions très complexes et tortueuses. Un plan bien étayé par des documents est nécessaire à la mise en œuvre d'un réseau sans fil. Dans cette rubrique, nous présentons les éléments à prendre en considération dans la conception et la planification d'un réseau local sans fil.

Le calcul du nombre d'utilisateurs qu'un réseau local sans fil peut prendre en charge n'est pas des plus simples. Le nombre d'utilisateurs dépend de la structure géographique de votre installation (nombre d'entités et de périphériques présents dans un espace), des débits de données attendus par les utilisateurs (car les radiofréquences étant un support partagé, plus les utilisateurs sont nombreux, plus les conflits en matière d'utilisation des radiofréquences sont importants), de l'utilisation de canaux sans chevauchement par les multiples points d'accès présents dans un ensemble de services étendus, ainsi que des paramètres de puissance de transmission (qui sont limités par la réglementation locale). Vous disposerez d'une prise en charge des fonctions sans fil suffisante pour vos clients si vous planifiez votre réseau de telle sorte que la couverture en radiofréquences soit adaptée à la taille d'un ensemble de services étendus. L'examen détaillé des points à prendre en compte pour la planification d'un nombre déterminé d'utilisateurs n'est pas abordé dans ce cours.

Cliquez sur le bouton Plan dans la figure.

Au moment de planifier l'emplacement des points d'accès, vous ne pourrez peut-être pas simplement tracer les cercles de zone de couverture et les disposer sur un plan. Même si la zone de couverture circulaire approximative s'avère importante, il existe d'autres recommandations.



Si les points d'accès doivent utiliser le câblage existant ou s'il n'est pas possible d'en installer à certains endroits, notez ces emplacements sur le plan.

- Placez les points d'accès au-dessus des obstacles.
- Positionnez les points d'accès à la verticale près du plafond et au centre de chaque zone de couverture, si possible.
- Installez les points d'accès à des endroits où les utilisateurs sont appelés à travailler. Par exemple, les salles de conférence constituent généralement un emplacement plus approprié pour les points d'accès que les couloirs.

Lorsque ces éléments ont été résolus, évaluez la zone de couverture attendue de chaque point d'accès. Cette valeur varie en fonction de la ou des normes de réseau local sans fil que vous déployez, de la nature de l'installation, de la puissance de transmission pour laquelle le point d'accès est configuré, etc. Veillez toujours à consulter les spécifications du point d'accès au moment de planifier les zones de couverture.

En vous servant de votre plan, placez les points d'accès sur le plan d'étage en faisant en sorte que les cercles de couverture se chevauchent, comme le montre l'exemple suivant.

Exemple de calcul

L'auditorium ouvert (bâtiment de type entrepôt/fabrication) illustré dans cette figure représente une surface approximative de 6 000 mètres carrés.

D'après les spécifications du réseau, chaque zone de service de base (BSA) doit disposer d'un débit 802.11b minimal de 6 Mbits/s, car la fonction de voix sur réseau LAN sans fil a été mise en œuvre sur ce réseau. Les points d'accès permettent d'atteindre un débit de 6 Mbits/s dans des zones ouvertes telles que celles représentées sur le plan, avec une zone de couverture de 1 500 mètres carrés dans bon nombre d'environnements.

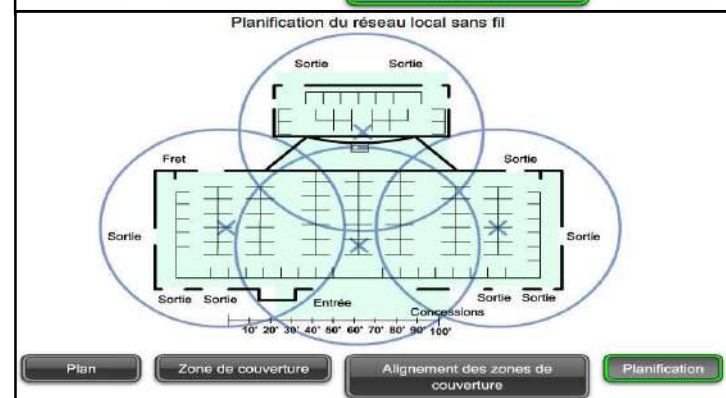
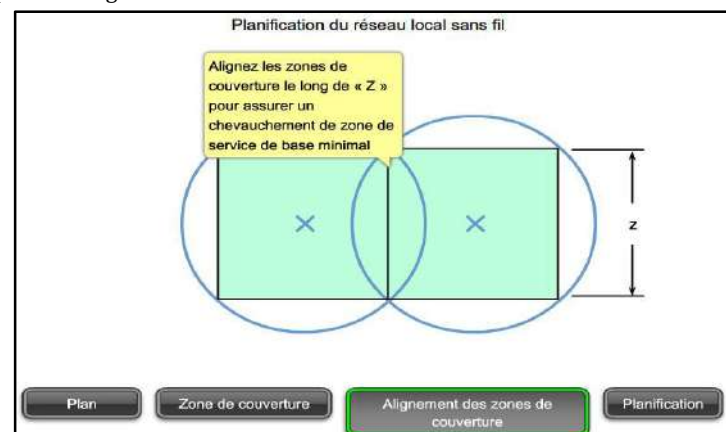
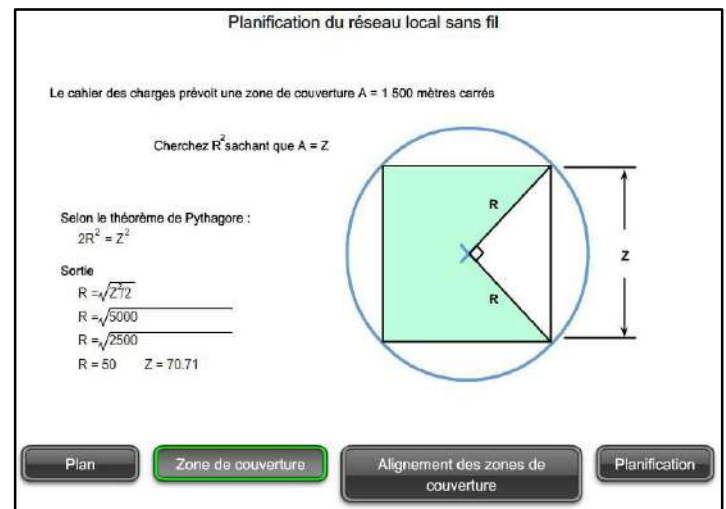
Remarque : la zone de couverture de 1 500 mètres carrés vaut pour un périmètre de forme carrée. Le rayon de la zone de service de base part en diagonale du centre de ce carré.

Déterminons l'emplacement des points d'accès.

Cliquez sur le bouton Zone de couverture dans la figure.

Sachant que l'installation représente une surface de 6 000 mètres carrés, si l'on divise cette surface par 1 500, qui représente la zone de couverture requise pour chaque point d'accès, le nombre de points d'accès nécessaires pour l'auditorium est d'au moins quatre unités. Ensuite, déterminons la dimension des zones de couverture et disposons-les sur le plan d'étage.

- La zone de couverture étant un carré avec un côté « Z », le cercle tangent à ses quatre angles présente un rayon de 15 mètres, comme le montrent les calculs.
- Une fois que les dimensions de la zone de couverture ont été déterminées, il convient de les disposer de la même façon que dans la figure (bouton Alignement des zones de couverture). **Cliquez sur le bouton Alignement des zones de couverture dans la figure.**
- Sur votre plan d'étage, disposez quatre cercles de couverture d'un rayon de 15 mètres en faisant en sorte qu'ils se chevauchent, comme illustré dans la figure (bouton Planification). **Cliquez sur le bouton Planification dans la figure. Page 2**



7.2-Sécurité des Réseaux Locaux Sans Fil

7.2.1-Menaces de Sécurité sur les Réseaux Locaux Sans Fil

Page 1 :

Accès non autorisé

La sécurité doit être une priorité pour tout utilisateur ou administrateur de réseaux. La difficulté de préserver la sécurité d'un réseau filaire est amplifiée avec un réseau sans fil. Un réseau local sans fil est ouvert à toute personne qui se trouve à portée d'un point d'accès et qui dispose des identifiants appropriés pour s'y associer. Moyennant une carte réseau sans fil et une connaissance des techniques de piratage, un pirate n'a pas forcément besoin de pénétrer physiquement dans l'espace de travail pour pouvoir accéder à un réseau local sans fil.

Dans cette première rubrique de la section présente, nous expliquons la façon dont les menaces de sécurité pesant sur les réseaux locaux sans fil ont évolué au fil du temps. Ces questions de sécurité sont même plus importantes dans le cas des réseaux d'entreprise, car la protection des données de l'entreprise est une condition même de sa pérennité. Pour une entreprise, les failles de sécurité peuvent avoir de graves répercussions, surtout si elle possède des informations financières relatives à ses clients.

Les catégories de menace pouvant conduire à un accès non autorisé sont essentiellement au nombre de trois :

- Pirates Wi-Fi
- Pirates informatiques
- Employés

À l'origine, le « piratage Wi-Fi » faisait référence à l'utilisation d'un appareil d'analyse dans le but de trouver des numéros de téléphone cellulaire à exploiter. Aujourd'hui, on appelle également piratage Wi-Fi le fait de chercher à exploiter un système 802.11b/g non sécurisé avec un ordinateur portable et une carte client 802.11b/g dans un voisinage.

Le terme « pirate informatique » désignait à l'origine toute personne cherchant à s'introduire dans un système informatique de façon à analyser, voire exploiter à des fins créatives, la structure et la complexité dudit système. De nos jours, ce terme désigne les intrus malveillants qui s'introduisent dans les systèmes en criminels dans le but de s'emparer de données ou d'endommager délibérément les systèmes. Les pirates résolus à causer des dommages sont capables d'exploiter les dispositifs de sécurité déficients.

La plupart des périphériques sans fil vendus aujourd'hui sont compatibles WLAN. En d'autres termes, les périphériques sont livrés avec des paramètres par défaut qui permettent aux utilisateurs de les installer et de les utiliser moyennant une configuration succincte, voire nulle. Or, souvent, soit les utilisateurs finaux ne modifient pas les paramètres par défaut, ce qui laisse la voie libre à une authentification client, soit ils sont simplement en mesure de mettre en œuvre la sécurité WEP standard. Hélas, comme nous l'avons indiqué précédemment, les clés WEP partagées sont défectueuses et donc faciles à pirater.

Certains outils conçus à des fins légitimes, tels que les sniffers sans fil, permettent aux ingénieurs réseau de capturer les paquets de données à des fins de débogage système. Ces mêmes outils peuvent être utilisés par des intrus pour exploiter les failles de sécurité.

Points d'accès non autorisés

Un point d'accès non autorisé est un point d'accès placé sur un réseau local sans fil dans le but de perturber le fonctionnement normal du réseau. Si un point d'accès non autorisé est configuré avec les paramètres de sécurité appropriés, les données client peuvent être capturées. Un point d'accès non autorisé peut également être configuré pour fournir à des utilisateurs non autorisés des informations telles que les adresses MAC de clients (sans fil et filaires), pour capturer et dénaturer des paquets de données voire, au pire, pour accéder à des serveurs et des fichiers.

Un exemple simple et courant de point d'accès non autorisé est celui qu'installent des employés sans autorisation, la motivation de ces employés étant de profiter du réseau d'entreprise à leur domicile. En règle générale, la configuration de sécurité de ces points d'accès est insuffisante, si bien que le réseau présente au final une faille de sécurité.

Pirates Wi-Fi	Pirates informatiques	Employés
Recherchent des réseaux « ouverts » pour accéder gratuitement à Internet	Exploitent les dispositifs de sécurité déficients pour consulter des informations confidentielles sur un réseau local sans fil, voire pour accéder à ce dernier	Branchent des API/passereaux grand public sur des ports Ethernet de l'entreprise pour créer leur propre réseau local sans fil

Page 2 :

Attaques de l'intercepteur

L'un des actes de piratage les plus sophistiqués qu'un utilisateur non autorisé puisse commettre est celui que l'on appelle l'attaque de l'intercepteur (Man-in-the-Middle, ou MITM). Les pirates choisissent un hôte pour cible et se positionnent logiquement entre la cible et le routeur ou la passerelle de la cible. Dans un environnement de réseau local filaire, le pirate doit pouvoir accéder physiquement au réseau local de façon à insérer logiquement un périphérique dans la topologie. Dans le cas d'un réseau local sans fil, les ondes radio émises par les points d'accès peuvent fournir la connexion.

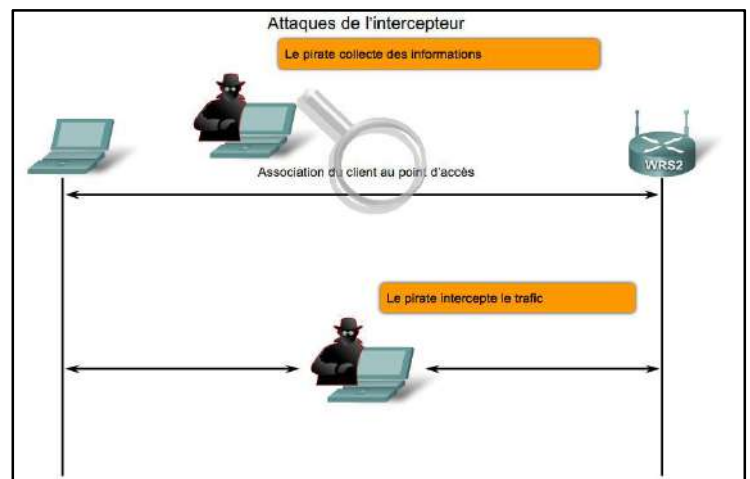
Les signaux radio des stations et des points d'accès sont « audibles » par toute personne qui dispose dans un ensemble de services de base de l'équipement adéquat, par exemple, d'un ordinateur portable équipé d'une carte réseau. Étant donné que les points d'accès agissent comme des concentrateurs Ethernet, chaque carte réseau au sein d'un ensemble de services de base entend tout le trafic. Le périphérique ignore le trafic qui ne lui est pas adressé. Les pirates peuvent modifier la carte réseau de leur ordinateur portable à l'aide d'un logiciel spécial de sorte qu'il accepte tout le trafic. Une fois cette modification effectuée, le pirate peut lancer des attaques MITM sur le réseau sans fil en utilisant la carte réseau de l'ordinateur portable comme point d'accès.

Pour mener à bien cette attaque, le pirate choisit une station pour cible et utilise un logiciel d'analyse de paquets, tel que Wireshark, pour observer la station client se connecter à un point d'accès. Le pirate peut parvenir à lire et copier le nom d'utilisateur de la cible, le nom du serveur, l'adresse IP du client et du serveur, l'ID utilisé pour calculer la réponse, de même que la demande de confirmation et la réponse d'association, qui est transmise en texte clair entre la station et le point d'accès.

Si le pirate est en mesure de compromettre un point d'accès, il peut potentiellement compromettre tous les utilisateurs de l'ensemble de services de base. Le pirate peut surveiller tout un segment de réseau sans fil et infliger des dégâts à l'encontre de tout utilisateur qui y est connecté.

Les chances de déjouer une attaque de type MITM dépendent de la sophistication de votre infrastructure de réseau LAN sans fil et de votre empressement à surveiller l'activité sur le réseau. Cela passe dans un premier temps par le recensement des périphériques légitimes de votre réseau local sans fil. Pour ce faire, vous devez authentifier les utilisateurs de votre réseau LAN sans fil.

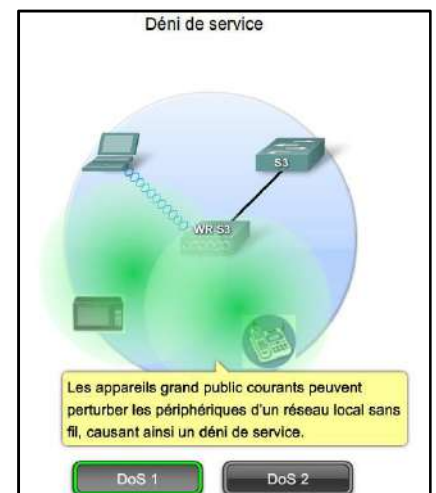
Une fois que tous les utilisateurs légitimes sont connus, vous surveillez le réseau pour repérer les périphériques et le trafic suspects. Les réseaux locaux sans fil d'entreprise dotés de périphériques WLAN de pointe procurent aux administrateurs des outils qui, ensemble, font office de système de protection contre les intrusions sur réseau local sans fil. Ces outils se composent notamment de dispositifs d'analyse, qui identifient les points d'accès non autorisés et les réseaux ad hoc, ou encore de systèmes de gestion des ressources radio, qui surveillent l'activité et la charge des points d'accès en analysant la bande RF. Un point d'accès plus actif que la normale peut être un signe pour l'administrateur qu'il existe du trafic non autorisé.



Page 3 :

Déni de service

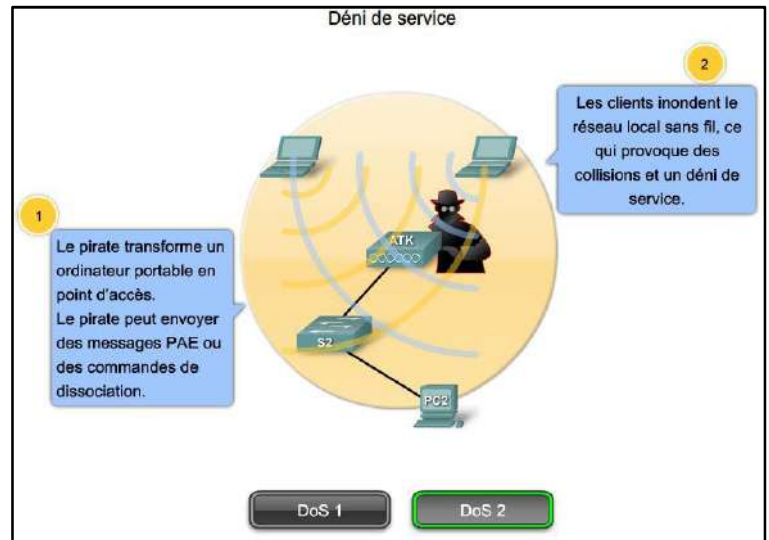
Les réseaux locaux sans fil de type 802.11b et g utilisent la bande ISM 2,4 GHz sans licence. Il s'agit de la même bande que celle utilisée par la plupart des produits sans fil grand public, comme les interphones bébé, les téléphones sans fil et les fours à micro-ondes. Face à l'encombrement de la bande RF par tous ces appareils, les pirates peuvent créer du bruit sur tous les canaux de la bande à l'aide de périphériques communs.



Cliquez sur le bouton DoS 2 dans la figure.

Nous avons vu précédemment comment un pirate pouvait transformer une carte réseau en point d'accès. Cette technique peut également servir à créer une attaque par déni de service (DoS). En utilisant un PC comme point d'accès, le pirate peut inonder l'ensemble de services de base de messages prêts à émettre (PAE) afin de neutraliser la fonction CSMA/CA utilisée par les stations. À leur tour, les points d'accès inondent l'ensemble de services de base de trafic simultané, ce qui provoque un flux constant de collisions.

L'autre moyen dont dispose un pirate pour lancer une attaque DoS dans un ensemble de services de base est d'envoyer une série de commandes de dissociation pour provoquer la déconnexion de toutes les stations dans l'ensemble de services de base. Après avoir été déconnectées, les stations tentent aussitôt de se réassocier, ce qui provoque une augmentation soudaine du trafic. Le pirate envoie une autre commande de dissociation et le cycle se répète.



7.2.2-Protocoles de sécurité sans fil

Page 1 :

Vue d'ensemble des protocoles sans fil

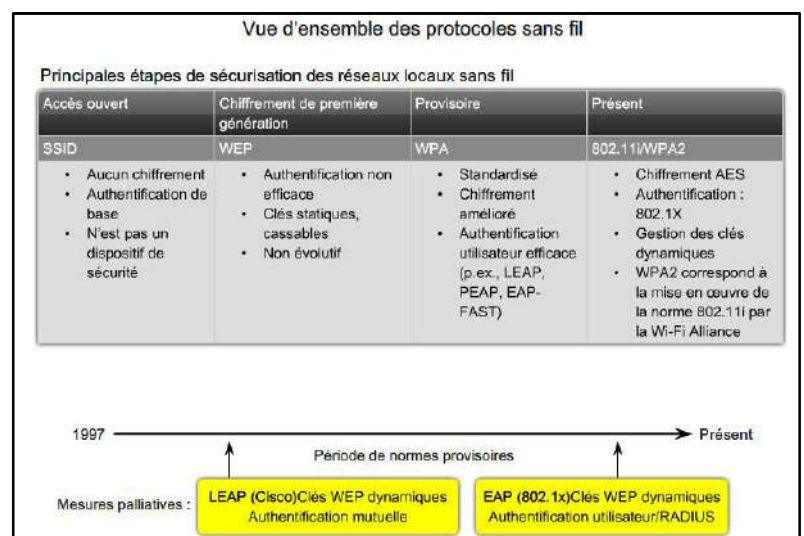
Dans cette rubrique, vous allez découvrir les caractéristiques des protocoles sans fil les plus courants, ainsi que le niveau de sécurité que chacun apporte.

La norme 802.11 d'origine avait établi deux types d'authentification : l'authentification par clé WEP ouverte et partagée. Si l'authentification ouverte correspond bel et bien à une non authentification (un client demande une authentification et le point d'accès la lui accorde), l'authentification WEP était censée assurer la confidentialité d'une liaison, à l'image d'un câble qui relie un PC à une prise murale Ethernet. Comme indiqué précédemment, les clés WEP partagées se sont avérées défectueuses et une meilleure solution s'imposait. Pour compenser les faiblesses de la clé WEP partagée, la toute première approche des sociétés a consisté à tester des techniques telles que le masquage des SSID et le filtrage d'adresses MAC. Ces techniques se sont également avérées trop faibles. Les faiblesses de ces techniques vous seront détaillées ultérieurement.

Les déficiences du chiffrement par clé WEP partagée étaient doubles. Tout d'abord, l'algorithme servant à chiffrer les données était cassable. Ensuite, l'autre problème concernait l'évolutivité. Les clés WEP 32 bits étant gérées manuellement, les utilisateurs les entraient par eux-mêmes, souvent de manière incorrecte, ce qui engendrait des appels au service d'assistance technique.

Suite au constat de faiblesse de la sécurité WEP, des mesures de sécurité provisoires ont vu le jour pendant un certain temps. À l'image de Cisco, certains fournisseurs désireux de répondre à des exigences de sécurité renforcée ont mis au point leurs propres systèmes tout en contribuant parallèlement à faire évoluer la norme 802.11i. Dans le cadre de l'élaboration de la norme 802.11i, l'algorithme de chiffrement TKIP fut créé, lequel était lié à la méthode de sécurité WPA (WiFi Protected Access) de la Wi-Fi Alliance.

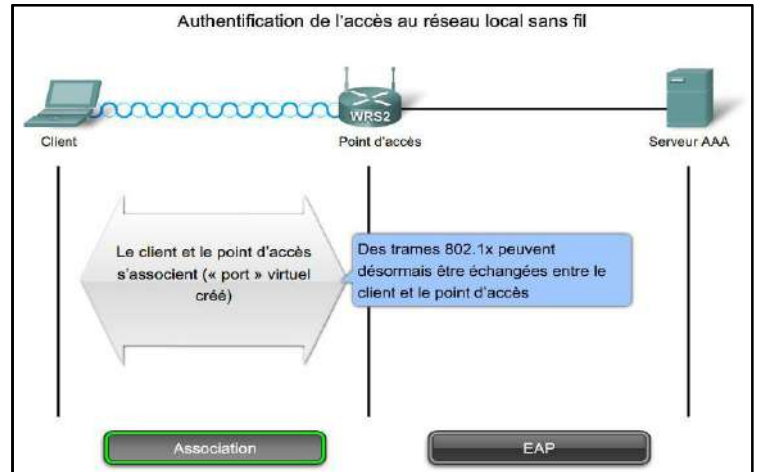
Aujourd'hui, la norme 802.11i est celle qui devrait faire foi dans la plupart des réseaux d'entreprise. Elle est comparable à la norme WPA2 de la Wi-Fi Alliance. Pour les entreprises, WPA2 inclut une connexion à une base de données RADIUS (Remote Authentication Dial In User Service). RADIUS est décrit plus loin dans ce chapitre.



Page 2 :

Authentification de l'accès au réseau local sans fil

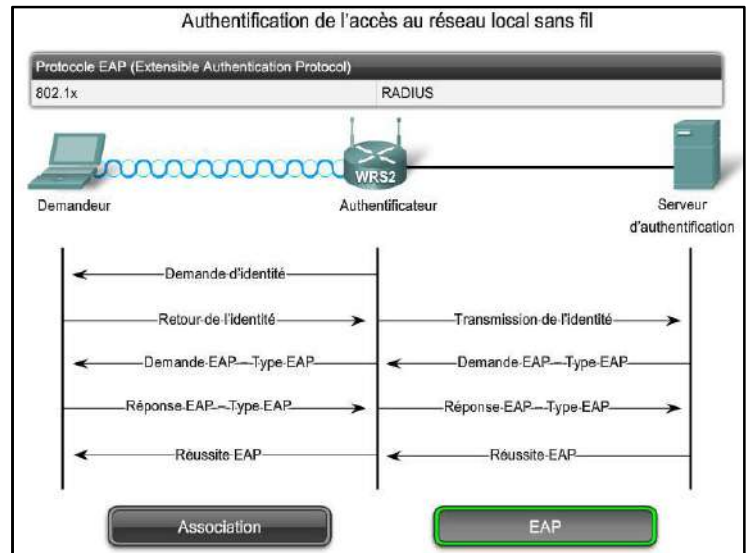
Dans un réseau ouvert, tel qu'un réseau domestique, les conditions d'octroi d'un accès client aux périphériques et aux services d'un réseau local peuvent se limiter à une simple association. Dans les réseaux où les exigences de sécurité sont plus strictes, l'octroi d'un tel accès aux clients passe par une authentification supplémentaire ou un ID de connexion. Ce processus de connexion est géré par le protocole EAP (Extensible Authentication Protocol). EAP est un protocole d'authentification de l'accès réseau. L'IEEE a développé la norme 802.11i pour l'authentification WLAN et l'autorisation d'utiliser la norme IEEE 802.1x.



Cliquez sur le bouton EAP dans la figure pour visualiser le processus d'authentification.

Le processus d'authentification dans le cadre des réseaux locaux sans fil d'entreprise peut être résumé comme suit :

- Le processus d'association 802.11 crée un port virtuel pour chaque client du réseau local sans fil au niveau du point d'accès.
- Le point d'accès bloque toutes les trames de données, à l'exception du trafic 802.1x.
- Les trames 802.1x acheminent via le point d'accès les paquets d'authentification EAP vers un serveur où sont gérés les identifiants d'authentification. Il s'agit d'un serveur d'authentification, d'autorisation et de comptabilisation (ou AAA) utilisant un protocole RADIUS.
- Si l'authentification EAP aboutit, le serveur AAA envoie un message de réussite EAP au point d'accès, lequel autorise alors le trafic de données en provenance du client WLAN à transiter par le port virtuel.
- Avant d'ouvrir le port virtuel, le chiffrement de la liaison de données entre le client WLAN et le point d'accès est établi pour garantir qu'aucun autre client WLAN ne peut accéder au port qui a été créé pour un client authentifié déterminé.



Avant que la norme 802.11i (WPA2) ou même WPA ne soit utilisée, certaines sociétés essayèrent de sécuriser leurs réseaux locaux sans fil en filtrant les adresses MAC et en ne diffusant pas de SSID. De nos jours, certains logiciels permettent de modifier facilement les adresses MAC associées aux cartes, si bien qu'il n'est pas compliqué de prendre le filtrage d'adresses MAC à contre-pied. Cela ne veut pas dire pour autant que vous ne devez pas y recourir, mais si vous employez cette méthode, vous devez l'accompagner d'autres mesures de sécurité, tels que WPA2.

Même si aucun SSID n'est diffusé par un point d'accès, le trafic échangé entre le client et le point d'accès finit par révéler le SSID. Si un pirate surveille passivement la bande RF, le SSID peut être sniffé dans l'une de ces transactions, car il est envoyé en texte clair. La facilité avec laquelle les SSID peuvent être découverts a conduit certaines personnes à laisser la diffusion de SSID activée. Il s'agit d'une décision qui doit être prise au niveau de l'organisation et qui doit figurer par écrit dans la stratégie de sécurité.

L'idée selon laquelle le filtrage MAC et la désactivation des diffusions de SSID suffisent à eux seuls à sécuriser un réseau local sans fil peut aboutir à une situation où le réseau est totalement vulnérable. Le meilleur moyen de s'assurer que les utilisateurs finaux se trouvent sur le réseau local sans fil est d'utiliser une méthode de sécurité qui intègre le contrôle d'accès réseau axé sur les ports, telle que WPA2.

Page 3 :

Chiffrement

Il existe deux mécanismes de chiffrement d'entreprise spécifiés par la norme 802.11i qui sont certifiés WPA et WPA2 par la Wi-Fi Alliance : le protocole TKIP (Temporal Key Integrity Protocol) et la norme AES (Advanced Encryption Standard).

Le protocole TKIP est la méthode de chiffrement certifiée WPA. Il offre une prise en charge de l'équipement de réseau LAN sans fil hérité en palliant les déficiences initiales inhérentes à la méthode de chiffrement WEP 802.11. Il utilise l'algorithme de chiffrement d'origine utilisé par WEP.

Le protocole TKIP remplit deux fonctions principales :

- Il chiffre les données utiles de couche 2.
- Il assure un contrôle d'intégrité des messages (MIC) dans le paquet chiffré. Cela constitue une garantie contre toute altération d'un message.

Même si TKIP pallie toutes les faiblesses connues de WEP, le chiffrement AES de WPA2 est la méthode à privilégier, car elle met les normes de chiffrement applicables aux réseaux locaux sans fil en phase avec les méthodes recommandées et des normes plus générales de l'industrie informatique, plus particulièrement la norme IEEE 802.11i.

TKIP – Temporal Key Integrity Key	AES – Advanced Encryption Standard
• Chiffrement par l'ajout de codage de bits de plus en plus complexe à chaque paquet • Basé sur le même algorithme de chiffrement (RC4) que WEP	• Nouvel algorithme de chiffrement utilisé dans 802.11i • Basé sur TKIP avec des fonctionnalités supplémentaires qui améliorent le niveau de sécurité offert

La norme AES assure les mêmes fonctions que TKIP, sauf qu'elle utilise d'autres données de l'en-tête MAC qui permettent aux hôtes de destination d'identifier si les bits non chiffrés ont été altérés. Elle ajoute également un numéro de séquence à l'en-tête des données chiffrées.

Lorsque vous configurez des points d'accès ou des routeurs sans fil Linksys, tels que le modèle WRT300N, il se peut que WPA ou WPA2 n'apparaissent pas, mais qu'il soit en revanche fait mention de ce que l'on appelle une clé pré-partagée (PSK). Il existe différents types de PSK, à savoir :

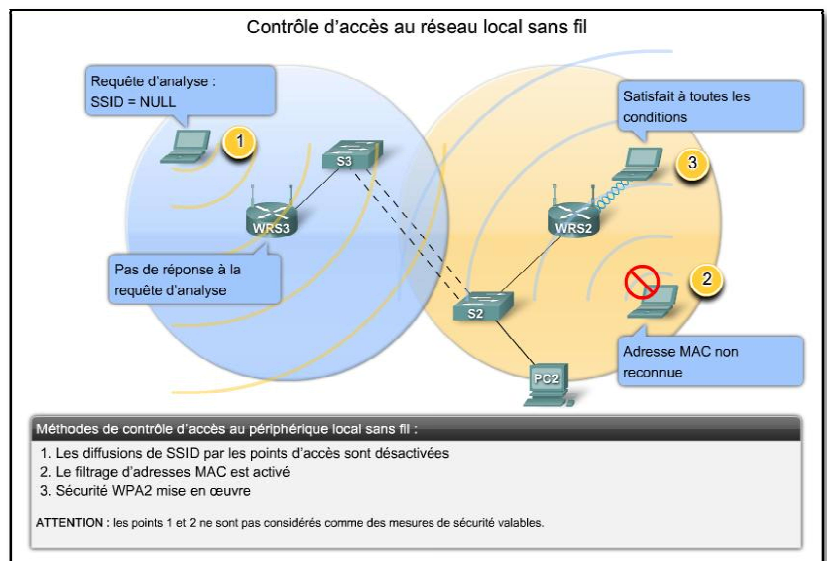
- PSK ou PSK2 couplé à TKIP est l'équivalent de WPA.
- PSK ou PSK2 couplé à AES est l'équivalent de WPA2.
- PSK2, sans méthode de chiffrement spécifiée, est l'équivalent de WPA2.

7.2.3-Sécurisation d'un Réseau local sans fil

Contrôle d'accès au réseau local sans fil

Le concept de profondeur signifie disposer de plusieurs solutions. C'est comme disposer d'un système de sécurité à votre domicile, et en outre verrouiller toutes les portes et les fenêtres et demander à vos voisins de le surveiller. Les méthodes de sécurité que nous vous avons présentées, notamment WPA2, assurent les fonctions d'un système de sécurité. Si vous souhaitez renforcer la sécurité d'accès à votre réseau local sans fil, vous pouvez ajouter de la profondeur, comme illustré dans la figure, en mettant en œuvre cette approche en trois étapes :

- Masquage de SSID - Les diffusions de SSID par les points d'accès sont désactivées
- Filtrage d'adresses MAC - Les tables sont construites manuellement au niveau du point d'accès pour autoriser ou refuser les clients en fonction de leur adresse matérielle physique
- Mise en œuvre de la sécurité de réseau local sans fil - WPA ou WPA2



Un autre élément important pour un administrateur réseau vigilant est de configurer les points d'accès proches des murs extérieurs du bâtiment de sorte que leur puissance de transmission soit inférieure à celle des autres points d'accès plus proches du centre du bâtiment. Ce paramétrage vise simplement à réduire la signature RF sur l'extérieur du bâtiment et ainsi à éviter que quelqu'un exécutant une application telle que Netstumbler (<http://www.netstumbler.com>), Wireshark, voire même Windows XP, ne puisse mapper les réseaux locaux sans fil.

Le masquage de SSID, pas plus que le filtrage d'adresses MAC, ne sont considérés comme des moyens fiables de sécuriser un réseau local sans fil pour les raisons suivantes :

- Il est facile d'usurper les adresses MAC.
- Il est facile de découvrir les SSID même si les points d'accès ne les diffusent pas.

7.3-Configuration de l'accès à un Réseau sans fil

7.3.1-Configuration du point d'accès sans fil

Page 1 :

Vue d'ensemble de la configuration du point d'accès sans fil

Dans cette rubrique, vous allez apprendre à configurer un point d'accès sans fil. Vous apprendrez à définir le SSID, à activer la sécurité, à configurer le canal et à ajuster les paramètres de puissance d'un point d'accès sans fil. Vous apprendrez également à sauvegarder et restaurer la configuration d'un point d'accès sans fil type.

Quand il s'agit de mettre en œuvre un réseau sans fil, ou tout autre réseau élémentaire, la méthode de base consiste à configurer et à tester par touches successives. Avant de mettre en œuvre des périphériques sans fil, vérifiez l'accès existant au réseau et à Internet des hôtes filaires. Démarrez le processus de mise en œuvre d'un réseau local sans fil avec un seul point d'accès et un seul client, sans activer la sécurité sans fil. Vérifiez que le client sans fil a reçu une adresse IP DHCP et qu'il peut envoyer une requête ping au routeur filaire local par défaut et qu'il peut accéder à Internet. Enfin, configurez la sécurité sans fil avec WPA2. N'utilisez WEP que si le matériel ne prend pas en charge WPA.

La plupart des points d'accès ont été conçus pour être prêts à l'emploi avec les paramètres par défaut. Toutefois, il est conseillé de modifier les configurations initiales par défaut. Nombreux sont les points d'accès qui peuvent être configurés via une interface graphique Web.

Une fois que vous avez un plan de mise en œuvre en tête, vérifiez la connectivité du réseau filaire et installez le point d'accès, vous devez ensuite le configurer. L'exemple suivant utilise un périphérique multifonction Linksys WRT300N. Ce périphérique intègre un point d'accès.

La procédure de configuration du Linksys WRT300N se compose des étapes suivantes :

Assurez-vous que votre PC est connecté au point d'accès via une connexion filaire, puis accédez à l'utilitaire Web à l'aide d'un navigateur Web. Pour accéder à l'utilitaire Web du point d'accès, lancez Internet Explorer ou Netscape Navigator, puis entrez l'adresse IP par défaut du WRT300N (192.168.1.1) dans le champ d'adresse. Appuyez sur Entrée.

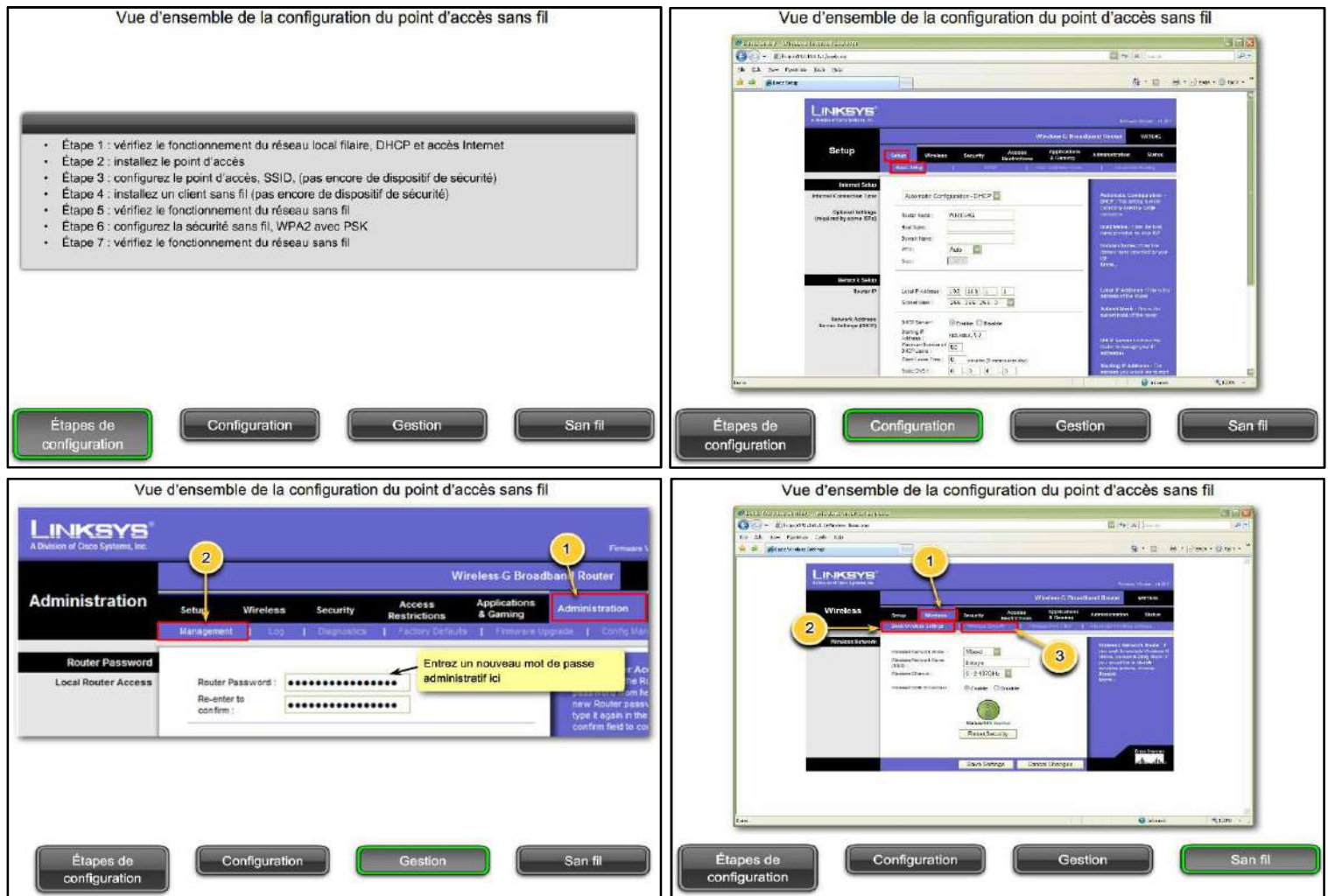
Un écran apparaît pour vous inviter à indiquer vos nom d'utilisateur et mot de passe. Laissez le champ Username (nom d'utilisateur) vide. Entrez **admin** dans le champ Password (mot de passe). Il s'agit des paramètres par défaut du Linksys WRT300N. Si le périphérique a déjà été configuré, il se peut que les nom d'utilisateur et mot de passe aient été modifiés. Cliquez sur **OK** pour continuer.

Pour une configuration réseau de base, utilisez les écrans suivants, tels qu'illustrés dans la figure lorsque vous **cliquez sur les boutons Configuration, Gestion et Sans fil** :

- **Configuration** - Entrez vos paramètres réseau de base (adresse IP).
- **Gestion** - Cliquez sur l'onglet **Administration** et sélectionnez l'écran Management. Le mot de passe par défaut est **admin**. Pour sécuriser le point d'accès, modifiez la valeur par défaut du mot de passe.
- **Sans fil** - Modifiez le SSID par défaut sous l'onglet **Basic Wireless Settings**. Sélectionnez le niveau de sécurité sous l'onglet **Wireless Security** et complétez les options en fonction du mode de sécurité choisi.

Apportez les modifications nécessaires via l'utilitaire. Après avoir apporté des modifications à un écran, cliquez sur le bouton **Save Settings** ou sur le bouton **Cancel** Changes pour annuler vos modifications. Pour plus d'informations sur un onglet, cliquez sur **Help**.

La figure récapitule les étapes de mise en œuvre d'un point d'accès.



Page 2 :

Configuration des paramètres sans fil de base

L'écran **Basic Setup** est le premier écran à s'afficher lorsque vous accédez à l'utilitaire Web. Cliquez sur l'onglet **Wireless** et sélectionnez l'onglet **Basic Wireless Settings**.

Paramètres sans fil de base

Cliquez sur les boutons alignés au bas de la figure pour obtenir une représentation de l'interface utilisateur pour chaque configuration.

- **Mode** (Network Mode) - Si votre réseau est équipé de périphériques sans fil N, G et 802.11b, conservez le paramètre par défaut, **Mixed**. Si vous disposez de périphériques sans fil G et 802.11b, sélectionnez l'option **BG-Mixed**. Si vous n'avez que des périphériques sans fil N, sélectionnez l'option **Wireless-N Only**. Si vous n'avez que des périphériques sans fil G, sélectionnez l'option **Wireless-G Only**. Si vous n'avez que des périphériques sans fil B, sélectionnez l'option **Wireless-B Only**. Si vous souhaitez désactiver la mise en réseau sans fil, sélectionnez **Disable**.
- **SSID** (Network Name (SSID)) - Le SSID correspond au nom de réseau partagé par tous les points d'un réseau sans fil. Il doit être identique pour tous les périphériques du réseau sans fil. Il est sensible à la casse et ne doit pas dépasser 32 caractères.

(vous pouvez utiliser n'importe quels caractères du clavier). Pour une sécurité accrue, vous avez tout intérêt à remplacer le SSID par défaut (linksys) par un nom unique.

SSID Broadcast - Lorsque les clients sans fil recherchent sur le réseau local les réseaux sans fil auxquels s'associer, ils détectent la diffusion du SSID par le point d'accès. Pour diffuser le SSID, conservez le paramètre par défaut, **Enabled**. Si vous ne voulez pas diffuser le SSID, sélectionnez **Disabled**. Après avoir apporté les modifications à cet écran, cliquez sur le bouton **Save Settings** ou sur le bouton **Cancel Changes** pour annuler vos modifications. Pour plus d'informations, cliquez sur Help.

- **Bande radio (Radio Band)** - Pour optimiser les performances dans un réseau utilisant des périphériques sans fil N, G et B, conservez le paramètre par défaut, **Auto**. Dans le cas des périphériques sans fil N uniquement, sélectionnez **Wide - 40MHz Channel**. Pour la mise en réseau de périphériques sans fil G et B uniquement, sélectionnez **Standard - 20MHz Channel**.
- **Canal large (Wide Channel)** - Si vous avez sélectionné l'option Wide - 40MHz Channel pour le paramètre **Radio Band**, ce paramètre est disponible pour votre canal sans fil N. Sélectionnez un canal dans le menu déroulant.
- **Canal standard (Standard Channel)** - Sélectionnez le canal pour la mise en réseau de périphériques sans fil N, G et B. Si vous avez sélectionné l'option Wide - 40MHz Channel pour le paramètre **Radio Band**, le canal standard est un canal secondaire pour périphérique sans fil N.

Configuration des paramètres sans fil de base



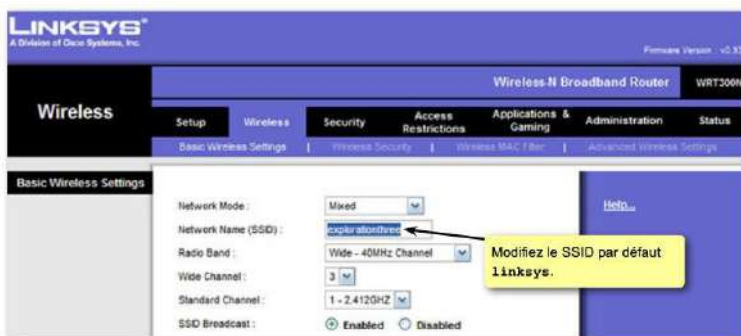
Vue d'ensemble Mode SSID Bande radio Canal large Canal standard

Configuration des paramètres sans fil de base



Vue d'ensemble Mode SSID Bande radio Canal large Canal standard

Configuration des paramètres sans fil de base

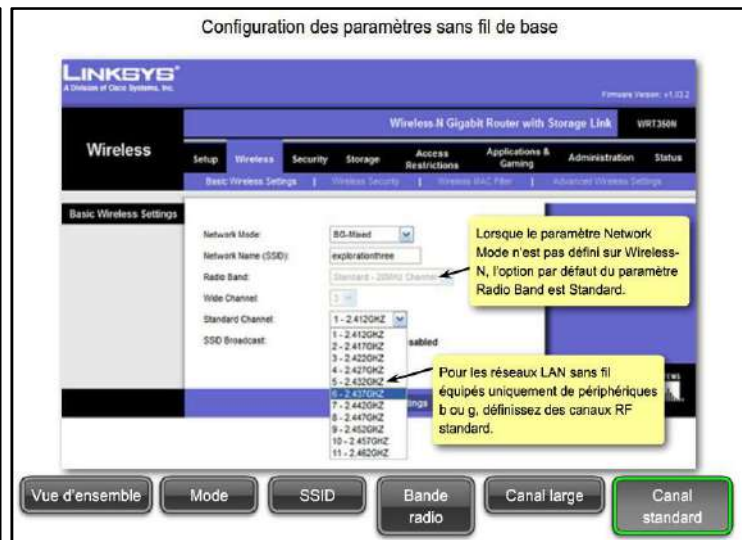


Vue d'ensemble Mode SSID Bande radio Canal large Canal standard

Configuration des paramètres sans fil de base



Vue d'ensemble Mode SSID Bande radio Canal large Canal standard



Page 3 :

Configuration de la sécurité

Cliquez sur le bouton *Vue d'ensemble* dans la figure.

Ces paramètres permettent de configurer la sécurité de votre réseau sans fil. Le WRT300N prend en charge sept modes de sécurité sans fil, ici répertoriés dans l'ordre de leur apparition dans l'interface graphique, du plus faible au plus fort, hormis la dernière option (Disabled) :

- WEP
- PSK-Personal ou WPA-Personal dans le progiciel v0.93.9 ou ultérieur
- PSK2-Personal ou WPA2-Personal dans le progiciel v0.93.9 ou ultérieur
- PSK-Enterprise ou WPA-Enterprise dans le progiciel v0.93.9 ou ultérieur
- PSK2-Enterprise ou WPA2-Enterprise dans le progiciel v0.93.9 ou ultérieur
- RADIUS
- Désactivé

Lorsqu'un mode de sécurité contient le mot « Personal », cela signifie qu'aucun serveur AAA n'est utilisé. La présence du mot « Enterprise » dans le nom du mode de sécurité indique qu'un serveur AAA et une authentification EAP sont utilisés.

Comme nous l'avons vu précédemment, WEP est un mode de sécurité déficient. PSK2, qui est l'équivalent de WPA2 ou IEEE 802.11i, est l'option à privilégier pour bénéficier d'une sécurité optimale. Si WPA2 est la meilleure option, vous devez vous demander pourquoi il en existe d'autres et en si grand nombre. Le fait est que bon nombre de réseaux locaux sans fil se composent de périphériques sans fil de générations précédentes. Or, tous les périphériques client qui s'associent à un point d'accès doivent utiliser le même mode de sécurité que ce dernier. Autrement dit, le point d'accès doit être défini de façon à prendre en charge le périphérique qui utilise le mode de sécurité le plus faible. Tous les périphériques de réseau LAN sans fil fabriqués après mars 2006 doivent pouvoir prendre en charge WPA2 ou, dans le cas des routeurs Linksys, PSK2. Ainsi, à terme, une fois que vous aurez mis à niveau vos périphériques, vous pourrez opter pour le mode de sécurité réseau PSK2.

L'option RADIUS, qui est accessible à un routeur sans fil Linksys, permet d'utiliser un serveur RADIUS conjointement avec WEP.

Cliquez sur les boutons alignés au bas de la figure pour obtenir une représentation de l'interface utilisateur pour chaque configuration.

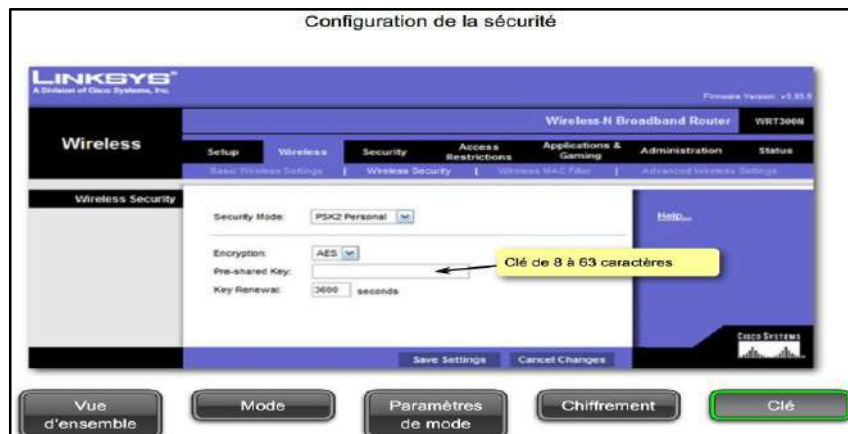
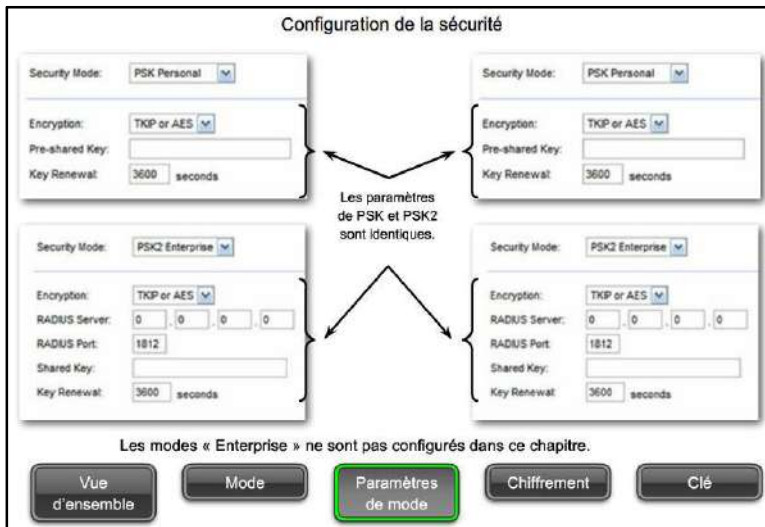
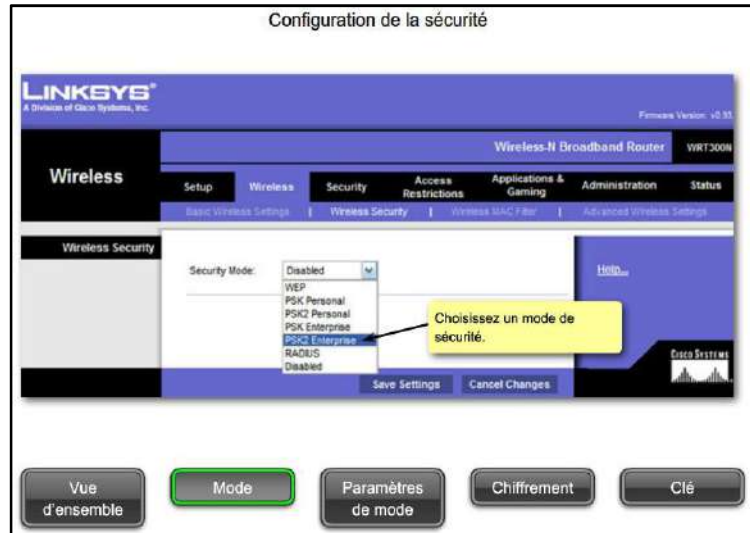
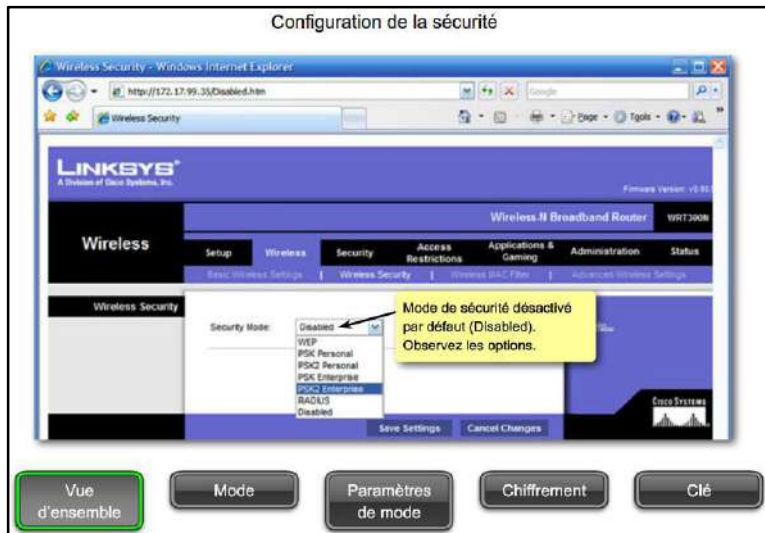
Pour configurer la sécurité, procédez comme suit :

- **Mode (Security Mode)** - Sélectionnez le mode que vous souhaitez utiliser : PSK-Personal, PSK2-Personal, PSK-Enterprise, PSK2-Enterprise, RADIUS ou WEP.
- **Paramètres de mode** - Les modes PSK et PSK2 proposent chacun des paramètres que vous pouvez configurer. Si vous sélectionnez le mode de sécurité PSK2-Enterprise, votre point d'accès doit être rattaché à un serveur RADIUS. Si vous avez opté pour cette configuration, vous devez configurer le point d'accès de sorte qu'il pointe vers le serveur RADIUS. Adresse

IP du serveur RADIUS (Radius Server) - Entrez l'adresse IP du serveur RADIUS. **Port du serveur RADIUS** (Radius Port) - Entrez le numéro de port utilisé par le serveur RADIUS. La valeur par défaut est de 1812.

- **Chiffrement (Encryption)** - Sélectionnez l'algorithme que vous voulez utiliser : AES ou TKIP. (La méthode de chiffrement AES est plus fiable que TKIP.)
- **Clé pré-partagée (Pre-shared Key)** - Entrez la clé partagée par le routeur et les autres périphériques de votre réseau. Elle doit comporter entre 8 et 63 caractères. **Renouvellement de clé (Key Renewal)** - Entrez la période de renouvellement de clé pour indiquer au routeur la fréquence de remplacement des clés de chiffrement.

Après avoir apporté les modifications à cet écran, cliquez sur le bouton **Save Settings** ou sur le bouton **Cancel Changes** pour annuler vos modifications.



7.3.2-Configuration d'une Carte Réseau sans fil

Page 1 :

Recherche de SSID

Une fois que le point d'accès a été configuré, vous devez configurer la carte réseau sans fil d'un périphérique client pour permettre à celui-ci de se connecter au réseau sans fil. Vous devez également vérifier que le client sans fil s'est correctement connecté au réseau sans fil voulu, surtout s'il existe plusieurs réseaux locaux sans fil auxquels il est possible de se connecter. Nous vous présenterons également certaines étapes de dépannage de base et identifierons les problèmes courants liés à la connectivité des réseaux locaux sans fil.

Si votre PC est équipé d'une carte réseau sans fil, vous êtes en principe en mesure de rechercher les réseaux sans fil. Les PC exécutant Microsoft Windows XP intègrent un moniteur de réseaux sans fil et un utilitaire client. Il se peut que vous ayez installé un autre utilitaire et que vous l'utilisiez de préférence à la version native de Microsoft Windows XP.

La procédure décrite ci-dessous indique comment utiliser la fonction d'affichage des réseaux sans fil propre à Microsoft Windows XP.

Cliquez sur les étapes numérotées dans la figure pour suivre ce processus.

Étape 1. Dans la Barre des tâches de Microsoft Windows XP, repérez l'icône de connexion réseau illustrée dans la figure. Double-cliquez sur cette icône pour accéder à la boîte de dialogue Connexions réseau.

Étape 2. Cliquez sur le bouton **Afficher les réseaux sans fil** de la boîte de dialogue.

Étape 3. Examinez les réseaux sans fil que votre carte réseau sans fil a réussi à détecter.

Si un réseau local ne figure pas dans la liste des réseaux, il est possible que vous ayez désactivé la diffusion de SSID sur le point d'accès. Auquel cas, vous devez entrer le SSID manuellement.

Page 2 :

Sélection du protocole de sécurité sans fil

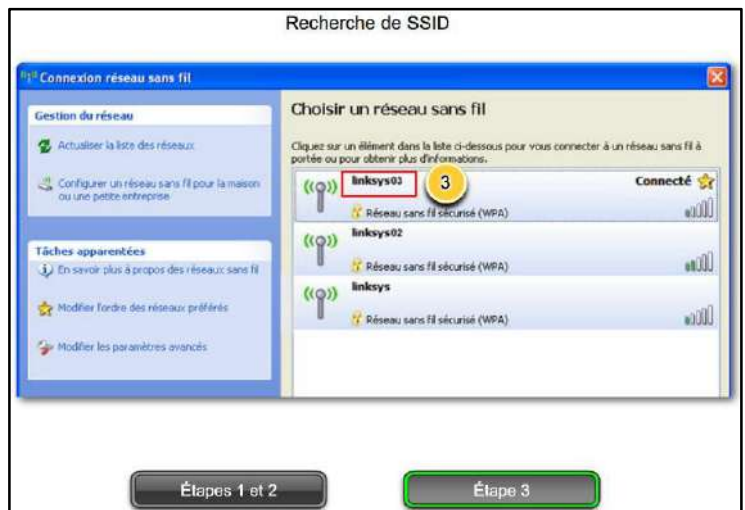
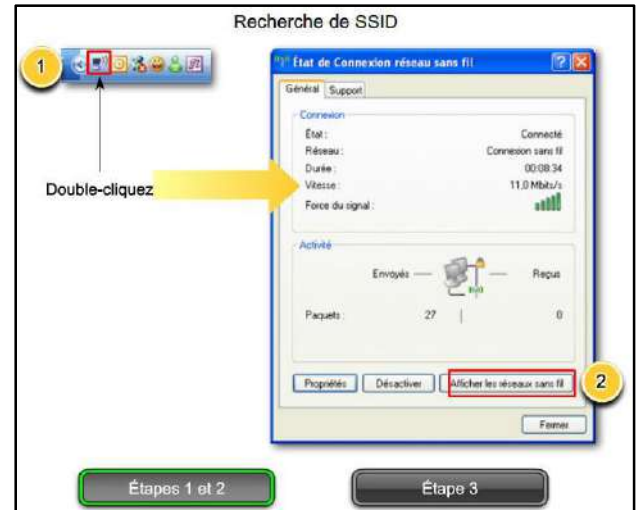
Après avoir configuré votre point d'accès de façon à authentifier les clients avec un type de sécurité fiable, vous devez faire correspondre la configuration de votre client avec les paramètres du point d'accès. La procédure suivante indique comment configurer les paramètres de sécurité de votre réseau sans fil sur le client :

Étape 1. Double-cliquez sur l'icône de connexion réseau dans la Barre des tâches de Microsoft Windows XP.

Étape 2. Cliquez sur le bouton **Propriétés** dans la boîte de dialogue Connexion réseau sans fil.

Étape 3. Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Configuration réseaux sans fil**.

Étape 4. Sous l'onglet **Configuration réseaux sans fil**, cliquez sur le bouton **Ajouter**. Vous pouvez également enregistrer plusieurs profils de réseau sans fil avec différents paramètres de sécurité pour vous permettre de vous connecter rapidement aux réseaux locaux sans fil que vous êtes appelé à utiliser régulièrement.



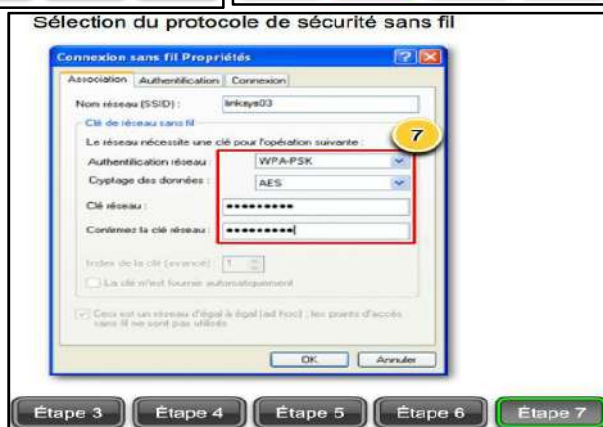
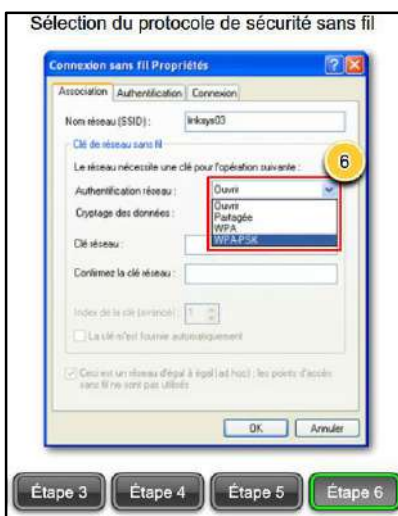
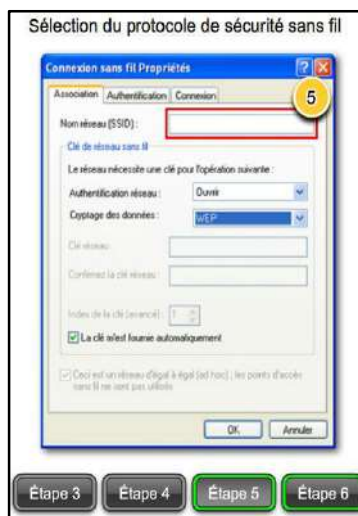
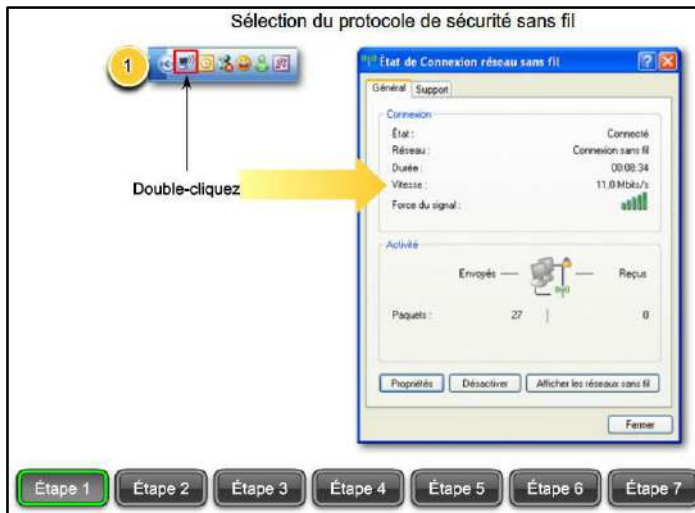
Étape 5. Dans la boîte de dialogue Propriétés du réseau sans fil, entrez le SSID du réseau local sans fil que vous souhaitez configurer.

Étape 6. Dans la zone Clé de réseau sans fil, sélectionnez votre méthode d'authentification préférée dans le menu déroulant **Authentification réseau**. WPA2 et PSK2 sont les méthodes à privilégier du fait de leur fiabilité.

Étape 7. Sélectionnez la méthode de **Cryptage des données** dans le menu déroulant. Pour rappel, l'algorithme de chiffrement AES est plus fiable que TKIP, mais vous devez ici faire correspondre la configuration de votre PC avec celle de votre point d'accès.

Après avoir sélectionné la méthode de cryptage (chiffrement), entrez et confirmez la **Clé réseau**. Encore une fois, il s'agit d'une valeur que vous avez entrée dans le point d'accès.

Étape 8. Cliquez sur **OK**.



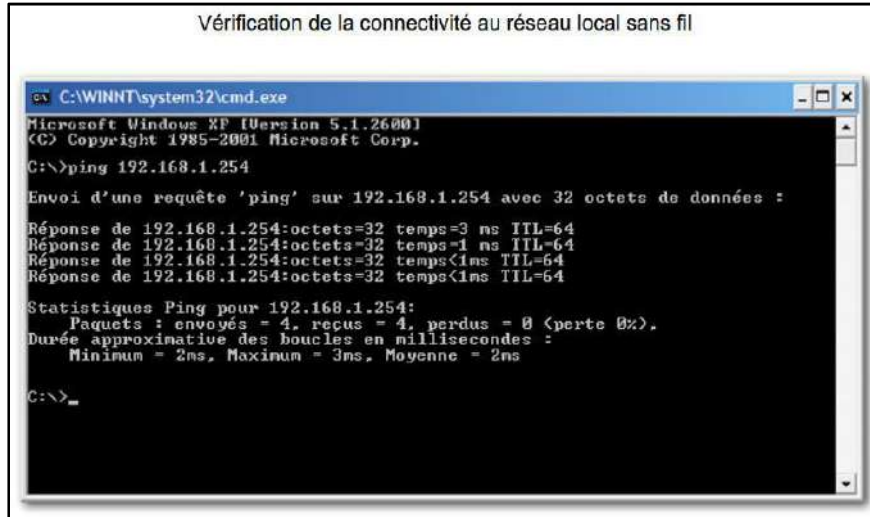
Page 3 :

Vérification de la connectivité au réseau local sans fil

Après avoir défini la configuration du point d'accès et du client, l'étape suivante consiste à vérifier la connectivité. Cette opération s'effectue en adressant une requête ping aux périphériques du réseau.

Ouvrez la fenêtre d'invite de commandes DOS sur le PC.

Essayez d'envoyer une requête ping à une adresse IP connue d'un périphérique du réseau. Dans la figure, l'adresse IP est 192.168.1.254. La requête ping a abouti, ce qui indique que la connexion a été établie.



```

C:\WINNT\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ping 192.168.1.254

Envoi d'une requête 'ping' sur 192.168.1.254 avec 32 octets de données :

Réponse de 192.168.1.254:octets=32 temps=3 ms TTL=64
Réponse de 192.168.1.254:octets=32 temps=1 ms TTL=64
Réponse de 192.168.1.254:octets=32 temps=1ms TTL=64
Réponse de 192.168.1.254:octets=32 temps=1ms TTL=64

Statistiques Ping pour 192.168.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%).
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\>_
  
```

7.4-Dépannage de problèmes simples liés aux Réseaux Locaux sans fil

7.4.1-Résolution des Problèmes radio et de logiciel au niveau des points d'accès

Page 1 :

Approche systématique du dépannage des réseaux locaux sans fil

Le dépannage d'un problème réseau, quelle que soit sa nature, doit obéir à une approche systématique, tout au long du parcours de la pile TCP/IP, depuis la couche physique jusqu'à la couche application. Cela permet d'éliminer les problèmes que vous êtes en mesure de résoudre par vous-même.

Cliquez sur le bouton **Méthode** dans la figure.

Vous devez déjà connaître les trois premières étapes de l'approche de dépannage systématique de réseaux locaux Ethernet 802.3. Elles sont reprises ici dans le contexte du réseau local sans fil :

Étape 1 - Élimination du PC de l'utilisateur comme source du problème

Essayez de déterminer la gravité du problème. En l'absence de connectivité, vérifiez les points suivants :

- Vérifiez la configuration réseau sur le PC à l'aide de la commande **ipconfig**. Vérifiez que le PC a reçu une adresse IP via le protocole DHCP ou qu'il est configuré avec une adresse IP statique.
- Vérifiez que le périphérique peut se connecter au réseau filaire. Connectez le périphérique au réseau local filaire et envoyez une requête ping à une adresse IP connue.
- Vous serez peut-être amené à essayer une autre carte réseau sans fil. Si nécessaire, rechargez les pilotes ou le logiciel (selon le cas) pour le périphérique client.
- Si la carte réseau sans fil du client fonctionne, vérifiez le mode de sécurité et les paramètres de chiffrement du client. Si les paramètres de sécurité ne correspondent pas, le client ne peut pas accéder au réseau local sans fil.

Si le PC de l'utilisateur fonctionne mais que ses performances ne sont pas satisfaisantes, vérifiez les points suivants :

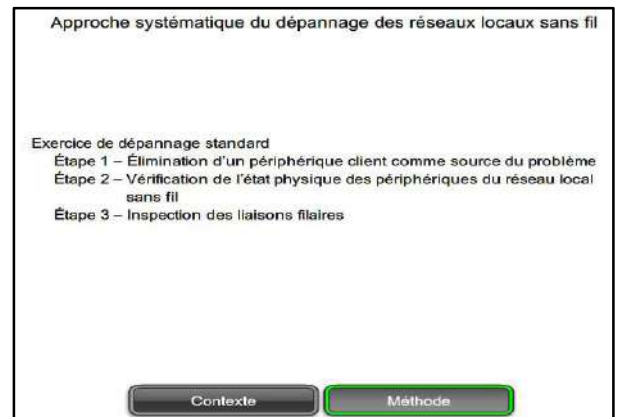
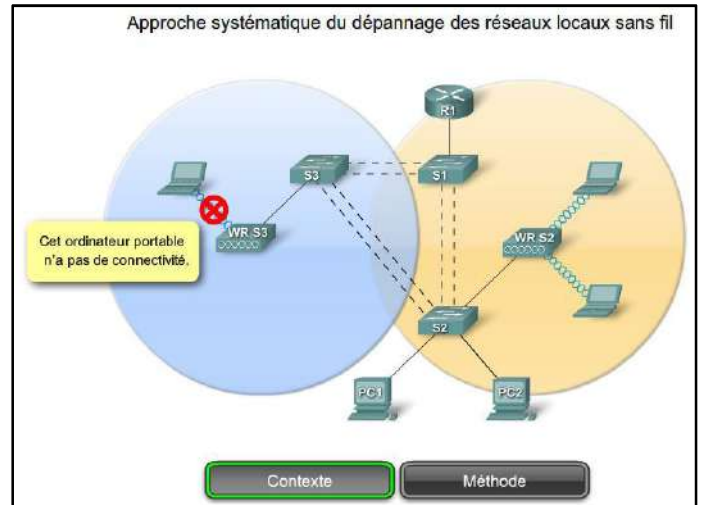
- Quelle est la distance qui sépare le PC d'un point d'accès ? Le PC se trouve-t-il en dehors de la zone de couverture prévue (BSA) ?
- Vérifiez les paramètres de canaux sur le client. Le logiciel client doit normalement détecter le canal approprié si le SSID est correct.
- Vérifiez si d'autres appareils utilisant la bande 2,4 GHz se trouvent dans la zone. Il peut s'agir notamment de téléphones sans fil, d'interphones bébé, de fours à micro-ondes, de systèmes de sécurité sans fil et de points d'accès non autorisés. Les données provenant de ces appareils peuvent provoquer des interférences dans le réseau local sans fil et des problèmes de connexion intermittents entre un client et un point d'accès.

Étape 2 - Vérification de l'état physique des périphériques

- Les périphériques sont-ils tous en place ? Envisagez l'existence d'un problème de sécurité physique.
- Les périphériques sont-ils tous alimentés en électricité et sont-ils sous tension ?

Étape 3 - Inspection des liaisons

- Inspectez les liaisons entre les périphériques câblés pour vous assurer que les connecteurs ne sont pas défectueux ou que les câbles ne sont pas endommagés ou manquants.
- Si l'infrastructure physique est en place, utilisez le réseau local filaire pour déterminer s'il est possible d'envoyer des requêtes **ping** aux périphériques, y compris au point d'accès.



Si il n'y a toujours pas de connectivité à ce stade, il se peut qu'un problème existe au niveau du point d'accès ou de sa configuration.

Lorsqu'il s'agit de dépanner un réseau local sans fil, il est conseillé de procéder par élimination, en envisageant toutes les possibilités, des éléments physiques jusqu'aux applications. Dès lors que vous avez écarté le PC de l'utilisateur comme source du problème et que vous avez également vérifié l'état physique des périphériques, penchez-vous sur le fonctionnement du point d'accès. Vérifiez l'alimentation électrique du point d'accès.

Si, après avoir vérifié les paramètres du point d'accès, la connexion radio est toujours défaillante, essayez de vous connecter à un autre point d'accès. Vous pouvez essayer d'installer de nouveaux pilotes radio ou un nouveau progiciel, procédure qui est expliquée à la suite.

Page 2 :

Mise à jour du progiciel du point d'accès Attention :

Attention : ne mettez à niveau le progiciel que si vous rencontrez des problèmes au niveau du point d'accès ou si la nouvelle version propose une fonction qui vous intéresse.

Le progiciel d'un périphérique Linksys, tel que celui qui est utilisé dans les travaux pratiques de ce cours, est mis à niveau à partir de l'utilitaire Web. Procédez comme suit :

Cliquez sur le bouton Télécharger le progiciel dans la figure.

Étape 1. Téléchargez le progiciel sur le Web. Pour un périphérique Linksys WTR300N, rendez-vous à l'adresse <http://www.linksys.com>.

Cliquez sur le bouton Sélectionner le progiciel à installer dans la figure.

Étape 2. Procédez à l'extraction du fichier du progiciel sur votre ordinateur.

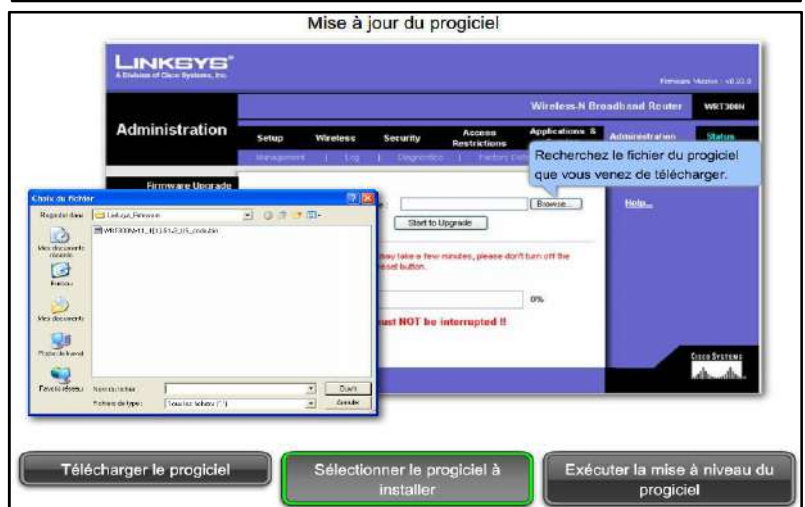
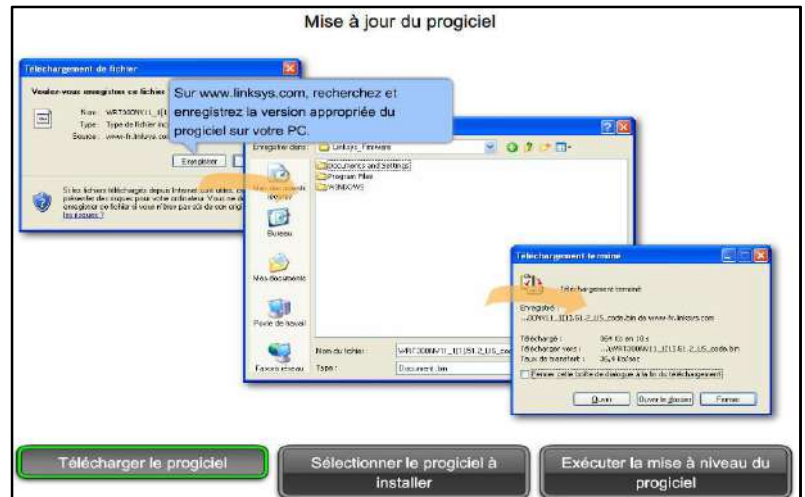
Étape 3. Ouvrez l'utilitaire Web, puis cliquez sur l'onglet **Administration**.

Étape 4. Sélectionnez l'onglet **Firmware Upgrade**.

Étape 5. Indiquez l'emplacement du fichier du progiciel ou cliquez sur le bouton Parcourir pour rechercher le fichier.

Cliquez sur le bouton Exécuter la mise à niveau du progiciel dans la figure.

Étape 6. Cliquez sur le bouton **Start to Upgrade** et suivez les instructions.



7.4.2-Paramètres des Canaux incorrects

Cliquez sur le bouton **Problème** dans la figure.

Si les utilisateurs font état de problèmes de connectivité dans la zone entre les points d'accès d'un réseau local sans fil compris dans un ensemble de services étendus, il se peut qu'il existe un problème de paramétrage des canaux.

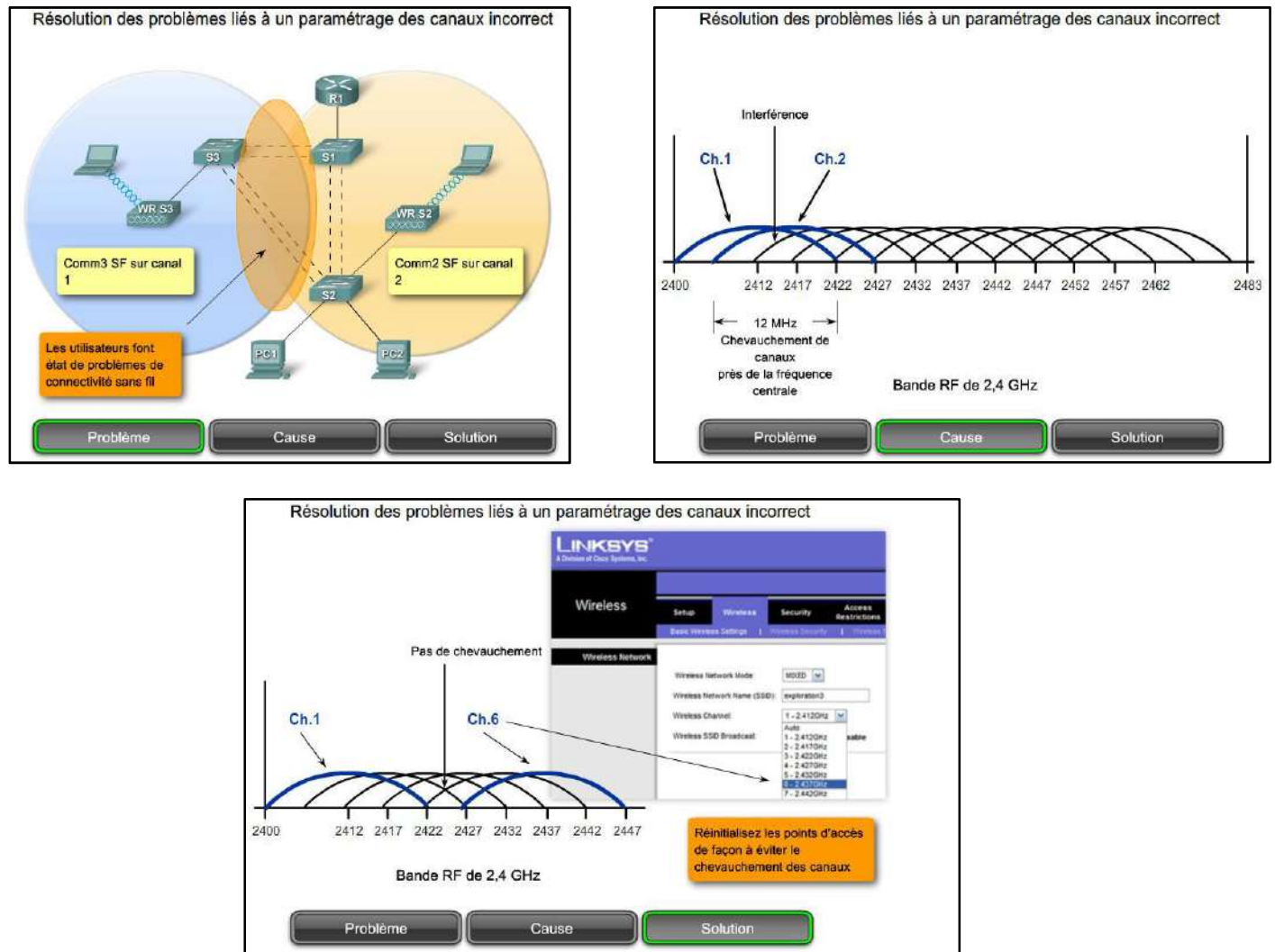
Cliquez sur le bouton **Cause** dans la figure.

La plupart des réseaux locaux sans fil d'aujourd'hui utilisent la bande 2,4 GHz, qui peut compter jusqu'à 14 canaux, chacun occupant 22 MHz de bande passante. L'énergie n'est pas répartie de manière uniforme sur la totalité des 22 MHz ; de fait, le canal est plus fort au niveau de sa fréquence centrale, tandis que l'énergie s'affaiblit vers ses extrémités. Le principe d'affaiblissement de l'énergie dans un canal est illustré par la ligne courbe représentant chaque canal. Le point haut au milieu de chaque canal est le point où l'énergie est la plus élevée. La figure fournit une représentation graphique des canaux de la bande 2,4 GHz.

La description détaillée du phénomène de répartition de l'énergie à travers les fréquences d'un canal sort du cadre de ce cours.

Cliquez sur le bouton **Solution** dans la figure.

Des interférences peuvent se produire en cas de chevauchement de canaux. Le cas le plus grave est lorsque les canaux se chevauchent à proximité des fréquences centrales, mais même en cas de chevauchement mineur, les signaux s'interfèrent entre eux. Définissez les canaux par intervalles de cinq (p. ex., canal 1, canal 6 et canal 11).



7.4.3-Résolution des Problèmes Radio et de logiciel au niveau des points d'accès

Résolution des interférences par radiofréquences

Le paramétrage incorrect des canaux fait partie d'un ensemble de problèmes plus général lié aux interférences par radiofréquences. Les administrateurs de réseaux locaux sans fil peuvent contrôler les interférences liées aux paramétrages des canaux par une planification efficace, notamment par un espacement approprié des canaux.

Cliquez sur le bouton Problème dans la figure.

D'autres sources d'interférences par radiofréquences existent tout autour de l'espace de travail ou à domicile. Peut-être l'avez-vous déjà remarqué, le signal de télévision peut être perturbé par le fonctionnement d'un aspirateur à proximité, qui se traduit par l'apparition de parasites à l'écran. De telles interférences peuvent être atténuées par une bonne planification. Par exemple, prévoyez de placer

les fours à micro-ondes à une certaine distance des points d'accès et des clients potentiels. Hélas, les problèmes d'interférences par radiofréquences ne peuvent pas tous être anticipés, du fait de la multitude de cas de figure possibles.

Cliquez sur le bouton Cause dans la figure.

Le problème posé par les appareils du type téléphones sans fil, interphones bébé et autres fours à micro-ondes est lié au fait qu'ils ne font pas partie d'un ensemble de services de base. Si bien qu'au lieu de rivaliser pour l'utilisation du canal, ils l'utilisent bel et bien. Comment identifier dans un réseau local les canaux les plus encombrés ?

Dans un environnement de réseau local sans fil de petite taille, essayez d'attribuer au point d'accès de votre réseau local sans fil le canal 1 ou le canal 11. Les appareils de consommation courante, tels que les

téléphones sans fil, utilisent souvent le canal 6.

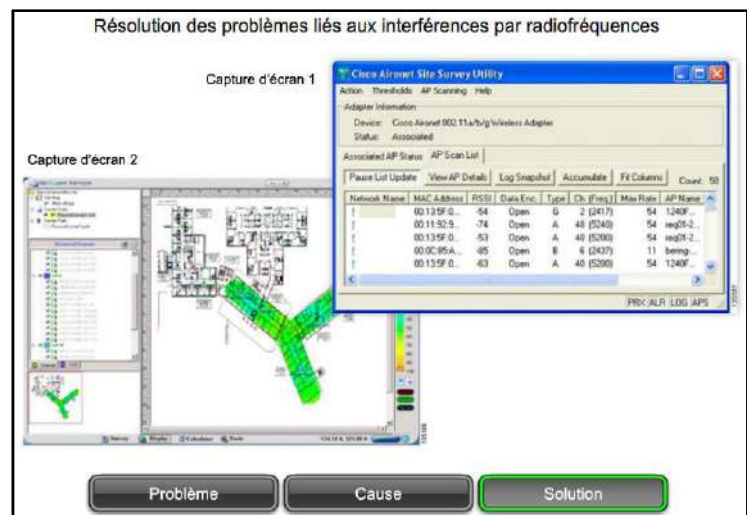
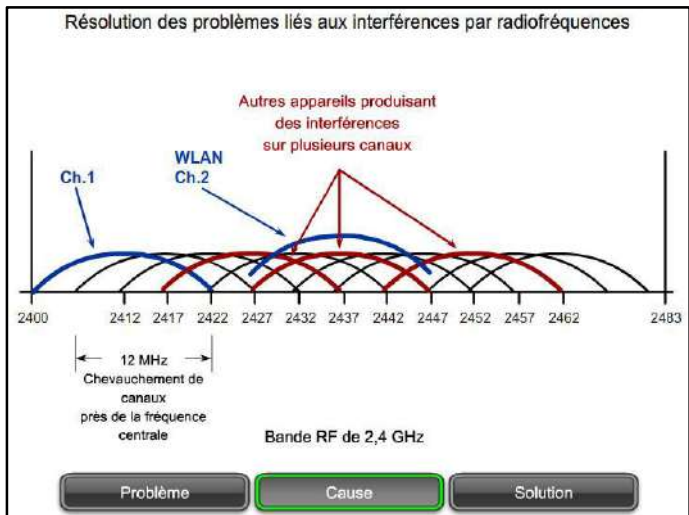
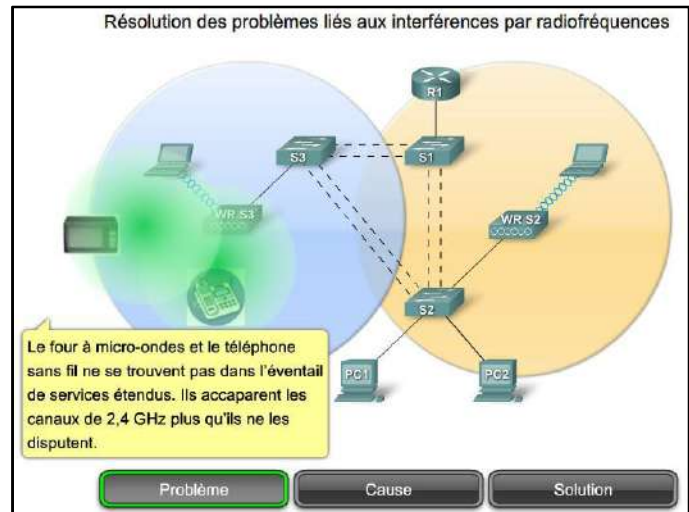
Études de site

Dans les environnements plus denses, une étude de site peut s'avérer indispensable. Vous ne serez certes pas amené à effectuer d'étude de site dans le cadre de ce cours, mais vous devez savoir qu'il existe deux types d'études de site : une manuelle et une assistée par un utilitaire.

Les études de site manuelles peuvent être assorties d'une évaluation de site, qui doit être suivie d'une étude de site plus approfondie avec l'aide d'un utilitaire. Une évaluation de site revient à inspecter la zone dans le but d'identifier les problèmes potentiels pouvant avoir un impact sur le réseau. Concrètement, cela consiste à rechercher la présence de plusieurs réseaux locaux sans fil, de structures de bâtiment uniques, telles que planchers ouverts et atriums, et de fortes variations dans l'utilisation des clients liées, par exemple, à des différences dans les niveaux de dotation en personnel entre les équipes de jour et de nuit.

Cliquez sur le bouton Solution dans la figure.

Il existe plusieurs méthodes en matière d'études de site assistées par un utilitaire. Si vous n'avez accès à aucun outil d'étude de site dédié, tel que Airmagnet, vous ne pouvez pas monter les points d'accès sur trépieds et les installer à des emplacements que vous



jugez appropriés et en conformité avec le plan de site prévu. Une fois les points d'accès installés, vous pouvez parcourir l'installation en utilisant un compteur d'évaluation de site dans l'utilitaire client WLAN de votre PC, comme illustré dans la capture d'écran 1 de la figure.

Sinon, il existe aussi des outils sophistiqués qui vous permettent d'entrer le plan d'étage d'une installation. Vous pouvez alors lancer un enregistrement des caractéristiques RF du site, qui s'affichent ensuite sur le plan d'étage à mesure que vous vous déplacez dans les locaux avec votre ordinateur portable sans fil. À titre d'exemple, le résultat d'une étude de site Airmagnet vous est montré dans la capture d'écran 2 de la figure.

Les études de site à l'aide d'un utilitaire présentent notamment l'avantage de rendre compte de l'activité RF sur les différents canaux des différentes bandes sans licence (900 MHz, 2,4 GHz et 5 GHz), ce qui vous permet de choisir les canaux de votre réseau local sans fil, ou du moins de repérer les zones de forte activité RF, et de prendre des dispositions en rapport.

7.4.4- Résolution des Problèmes Radio et de logiciel au niveau des points d'accès

Identification des problèmes liés au mauvais positionnement des points d'accès

Dans cette rubrique, vous allez apprendre à déterminer lorsqu'un point d'accès est mal placé et comment le positionner correctement dans une petite ou moyenne entreprise.

Cliquez sur le bouton Problème dans la figure.

Peut-être avez-vous déjà eu cette impression qu'un réseau local sans fil ne fonctionnait pas aussi bien qu'il le devrait. Vous n'avez pas cessé de perdre l'association à un point d'accès ou vos débits de données étaient plus faibles que la normale. Vous avez peut-être même fait le tour de votre installation pour vérifier que les points d'accès étaient bel et bien là. En constatant leur présence, vous vous êtes demandé pourquoi la qualité du service était toujours aussi mauvaise.

Cliquez sur le bouton Cause dans la figure.

Deux problèmes de déploiement majeurs liés à l'emplacement des points d'accès peuvent exister :

- La distance séparant les points d'accès est trop importante pour permettre une couverture par chevauchement.
- L'orientation des antennes des points d'accès situés dans les couloirs et les encoignures réduit la couverture.

Cliquez sur le bouton Solution dans la figure.

Pour résoudre le problème lié à l'emplacement des points d'accès, procédez comme suit :

Vérifiez les paramètres de puissance de transmission et la portée opérationnelle des points d'accès et disposez-les de façon à obtenir un chevauchement de cellules compris au minimum entre 10 et 15 %, comme nous l'avons vu dans ce chapitre.

Modifiez l'orientation et le positionnement des points d'accès :

- Placez les points d'accès au-dessus des obstacles.
- Positionnez les points d'accès à la verticale près du plafond et au centre de chaque zone de couverture, si possible.
- Installez les points d'accès à des endroits où les utilisateurs sont appelés à travailler. Par exemple, les grandes salles constituent généralement un emplacement plus approprié pour les points d'accès que les couloirs.

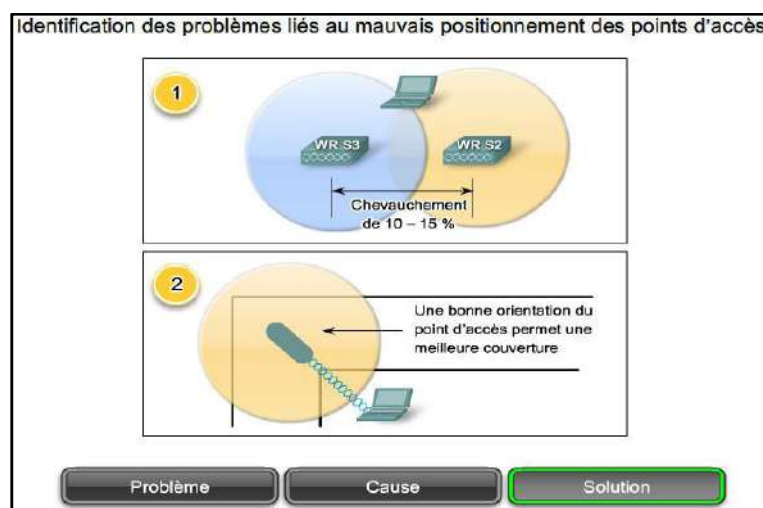
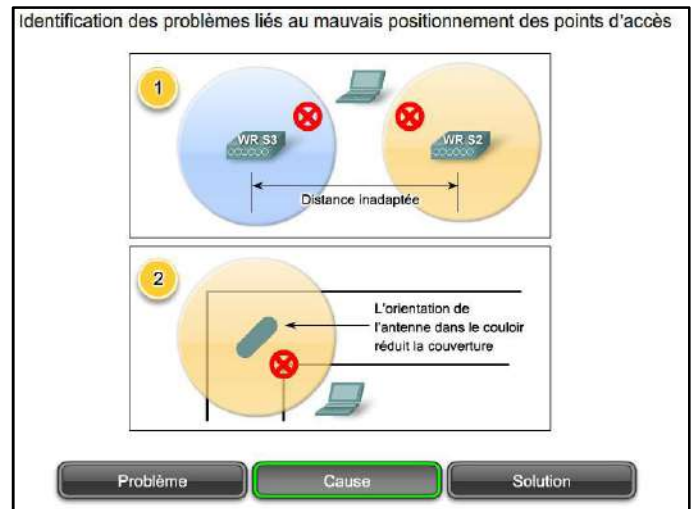
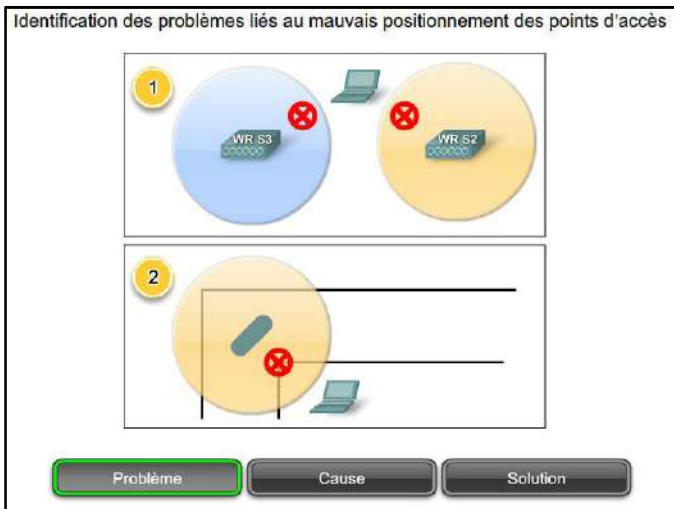
La figure explore ces questions à travers trois étapes successives : problème, cause, solution.

Cliquez successivement sur chaque bouton pour avancer dans le graphique.

D'autres points doivent être pris en compte concernant l'emplacement des points d'accès et des antennes :

- Assurez-vous que les points d'accès ne sont pas installés à moins de 20 cm du corps des personnes.
- Évitez de placer les points d'accès à moins de 90 cm d'obstacles métalliques.
- N'installez pas les points d'accès à proximité de fours à micro-ondes. Les fours à micro-ondes utilisant la même fréquence que les points d'accès, des signaux parasites peuvent se produire.
- Veillez à toujours installer le point d'accès à la verticale (posé ou en suspension).
- N'installez pas le point d'accès à l'extérieur des bâtiments.

- Ne placez pas les points d'accès près des murs extérieurs d'un bâtiment, à moins que vous souhaitiez offrir une couverture extérieure.
- Lorsque vous installez un point d'accès dans une encoignure à l'intersection de deux couloirs, placez-le à 45 degrés par rapport aux deux couloirs. Les antennes internes des points d'accès ne sont pas omnidirectionnelles et couvrent une zone plus importante lorsqu'elles sont installées de cette façon.

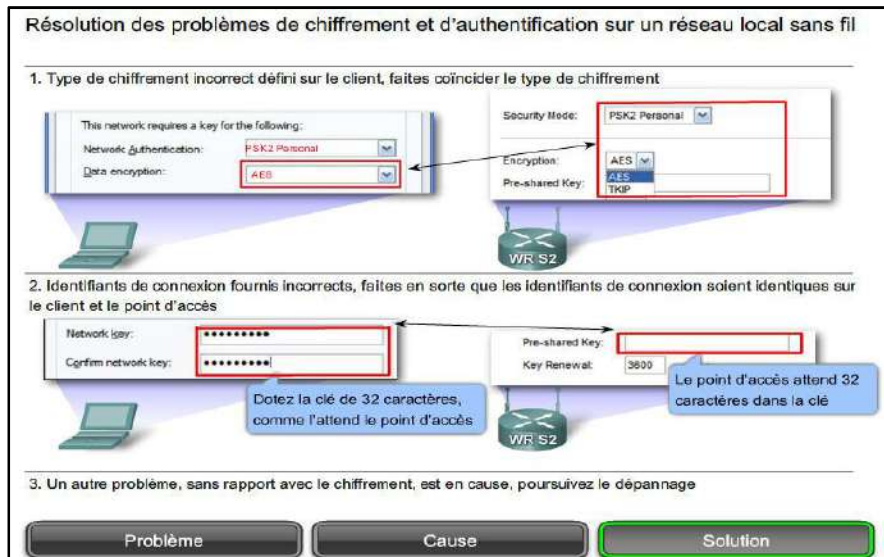
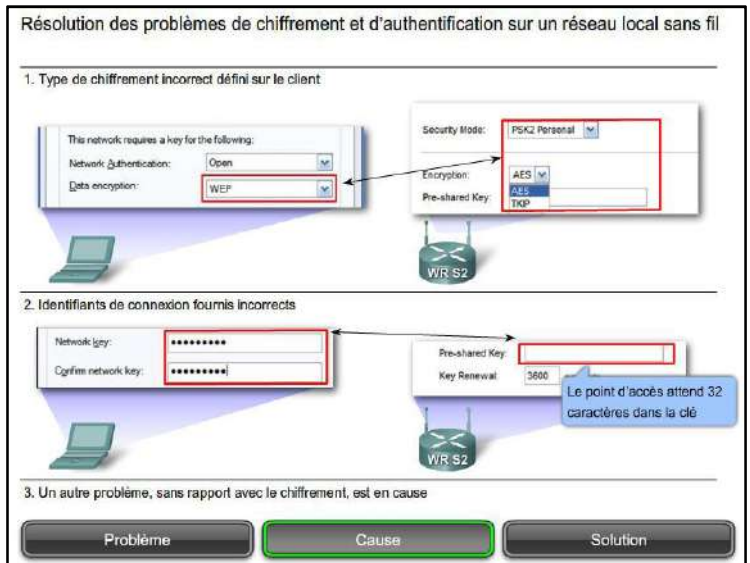
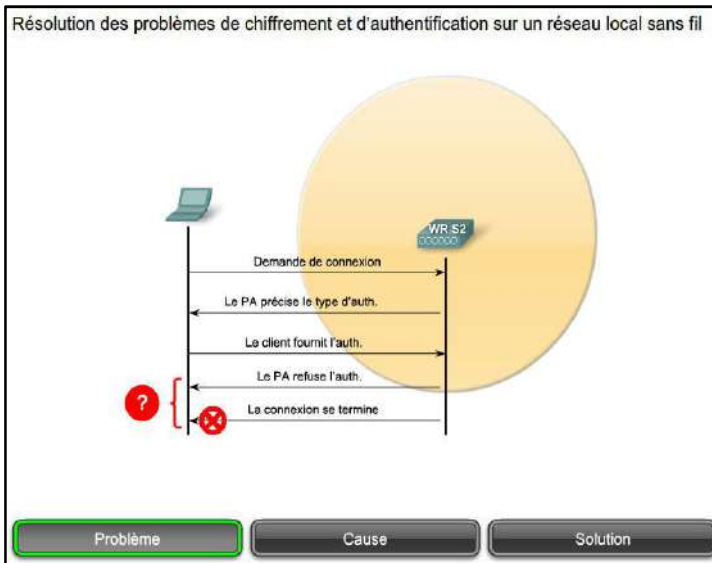


7.4.5-Problèmes d'Authentification et de Chiffrement

Les problèmes d'authentification et de chiffrement que vous êtes le plus susceptible de rencontrer sur un réseau local sans fil (et de résoudre par vous-même) sont le fait de paramètres client incorrects. Si un point d'accès attend un type de chiffrement et que le client en propose un autre, le processus d'authentification échouera.

Les problèmes de chiffrement impliquant la création de clés dynamiques ne sont pas abordés dans ce cours, pas plus que les conversations entre un serveur d'authentification, tel qu'un serveur RADIUS, et un client transitant par un point d'accès.

Pour rappel, tous les périphériques qui se connectent à un point d'accès doivent utiliser le même type de sécurité que celui configuré au niveau du point d'accès. Par conséquent, si un point d'accès est configuré pour le mode de sécurité WEP, le type de chiffrement (WEP) et la clé partagée doivent tous deux correspondre sur le client et le point d'accès. Si WPA est utilisé, l'algorithme de chiffrement est TKIP. De même, si WPA2 ou 802.11i est utilisé, AES est l'algorithme de chiffrement à utiliser.



7.6-Résumé

Dans ce chapitre, nous avons parlé des normes en constante évolution des réseaux locaux sans fil, notamment des normes IEEE 802.11a, b, g et n, qui est à l'état de projet. Les normes récentes prennent en compte la nécessité de prendre en charge la voix et la vidéo, ainsi que la qualité de service.

Le fait de connecter un point d'accès unique à un réseau local filaire permet de fournir aux stations client qui s'y associent un ensemble de services de base. Plusieurs points d'accès qui partagent un même identificateur d'ensemble de services constituent un ensemble de services étendus. Les réseaux locaux sans fil peuvent être détectés par tout périphérique client capable de recevoir des signaux radio, ce qui les met à la portée des pirates qui ne peuvent pas accéder à un réseau exclusivement filaire.

Certaines méthodes, telles que le filtrage d'adresses MAC et le masquage de SSID, peuvent faire partie intégrante d'une mise en œuvre de Méthodes Recommandées en matière de sécurité. Toutefois, ces méthodes à elles seules ne peuvent pas résister à un pirate déterminé. L'authentification WPA2 et 802.1x offre un accès très sécurisé aux réseaux locaux sans fil d'un réseau d'entreprise.

Les utilisateurs finaux doivent configurer une carte réseau sans fil sur leur station client, qui communique avec un point d'accès sans fil et s'y associe. Pour que l'association entre le point d'accès et une carte réseau sans fil soit possible, tous deux doivent être configurés avec des paramètres identiques, notamment le SSID. Au moment de configurer un réseau local sans fil, assurez-vous que les périphériques disposent de la dernière version du progiciel pour permettre une prise en charge des options de sécurité les plus rigoureuses. Outre la nécessité de s'assurer que la configuration des paramètres de sécurité sans fil est compatible, le dépannage d'un réseau local sans fil suppose de résoudre les problèmes de radiofréquences.

Dans ce chapitre, vous avez appris les éléments suivants :

- Grâce aux normes en constante évolution que sont notamment les normes 802.11a, b, g et à présent n, qui est à l'état de projet, il est possible de déployer des applications puissantes, telles que la voix, en tant que services de mobilité sur les réseaux locaux sans fil.
- Le fait de connecter un point d'accès unique à un réseau local filaire permet de fournir aux stations client qui s'y associent un ensemble de services de base. Plusieurs points d'accès qui partagent un même identificateur d'ensemble de services constituent un éventail de services étendus.
- Les réseaux locaux sans fil peuvent être détectés par tout périphérique client capable de recevoir des signaux radio, ce qui les met à la portée des pirates qui ne peuvent pas accéder à un réseau exclusivement filaire.
- Certaines méthodes, telles que le filtrage d'adresses MAC et le masquage de SSID, peuvent faire partie intégrante des Méthodes Recommandées en matière de sécurité. Toutefois, ces méthodes à elles seules ne peuvent pas résister à un pirate déterminé. Un réseau local sans fil d'entreprise doit au minimum disposer d'une authentification PSK2 Entreprise couplée à 802.1x en guise de dispositif de sécurité.
- Pour que l'association entre un point d'accès et une carte réseau sans fil soit possible, tous deux doivent être configurés avec des paramètres identiques, notamment le SSID.
- Lorsque vous configurez un réseau local sans fil, assurez-vous que les périphériques disposent de la dernière version du progiciel de sorte que tous puissent être configurés correctement et avec les derniers paramètres disponibles, tels que PSK2 Entreprise.
- Si des périphériques sans fil se déconnectent du réseau local sans fil, vérifiez le paramétrage des canaux et cherchez la présence éventuelle d'interférences causées par des appareils tels que fours à micro-ondes et téléphones sans fil.